

# VNIVERSITAT Đ VALÈNCIA



FACULTAT DE FILOSOFIA I CIÈNCIES DE L'EDUCACIÓ  
DEPARTAMENT DE DIDÀCTICA I ORGANITZACIÓ ESCOLAR

PROGRAMA DE DOCTORADO EN EDUCACIÓ

(Código: 3117; RD. 99/2011)

TESIS DOCTORAL

**Digital safety. La noción de seguridad digital en los alumnos de la  
escuela secundaria de segundo grado**

**PRESENTADA POR:**

M<sup>a</sup> TIZIANA OCCHIPINTI

**DIRIGIDA POR:**

DR. ÀNGEL SAN MARTÍN ALONSO

DR. CRISTÓBAL SUÁREZ-GUERRERO

**València, mayo de 2021**



## **Agradecimientos**

No puedo concluir este trabajo sin dar las gracias a todos los que me han apoyado durante la larga investigación, recopilación y redacción de esta tesis.

En primer lugar, quiero agradecer a mis directores de tesis, el Dr. Ángel San Martín Alonso y el Dr. Cristóbal Suárez-Guerrero, su incondicional ayuda y dedicación a lo largo de estos años. Gracias a ellos pude completar esta investigación en la que tanto creía.

Gracias también a la Dra. Donatella Donato, que ha sido un faro en el interminable mar de obligaciones burocráticas, y un apoyo seguro en los momentos más difíciles.

Gracias al Dr. Giovanni Gianni, director médico de "Fisiomedica Ragusa" por su colaboración puntual y profesional.

Un afectuoso agradecimiento a la señora Addario, que me proporcionó un punto de vista estratégico en la observación de la dinámica de la clase.

Mi gratitud va, también y sobre todo, a los Directores de Escuela, el Prof. Giuseppe Galofaro del IIS E. Fermi de Vittoria y el Prof. Gaetano Zisa del Instituto Verga de Vittoria, que me han abierto generosamente las puertas de sus institutos para realizar mi investigación.

Agradezco al vicepresidente de Argo Software, el Dr. Fausto Vicari, la información técnico-informática que nos ha proporcionado con abundancia y profesionalidad.

Doy las gracias a mi marido Rocco por apoyarme y creer en mí, y a mi hijo Alessandro por ser mi motivación e inspiración. Les agradezco a ambos su paciencia durante los muchos meses de estudio.

Doy las gracias a mi padre Carmelo, que me enseñó a no tener miedo de las cuestas más empinadas y a amar el estudio de forma intensa y apasionada.

Gracias a mi madre por la abnegación que siempre ha tenido hacia mí y sin la cual nada hubiera sido posible.

Gracias a mi hermano Salvatore que, incluso en su dolorosa ausencia, ha desempeñado un papel crucial en mi vida y en mi educación.

Gracias a todos

# Índice

Índice de tablas .....	7
Resumen .....	10
<b>INTRODUCCIÓN</b> .....	12
1. El proyecto: la seguridad en línea .....	12
2. Propuesta de estudio.....	14

## PRIMERA PARTE

### FUNDAMENTACIÓN TEÓRICA

#### CAPÍTULO I

##### Revisión del estado de la cuestión

1.1. <i>Digital Literacy</i> .....	23
1.2. Educación y medios de comunicación: "afinidad electiva" .....	27
1.3. Riesgos y beneficios de la sociedad de la información .....	29
1.3.1. <i>Fake news</i> .....	32
1.3.2. Robo de datos .....	35
1.3.3. Acoso en línea .....	38
1.3.4. <i>Sexting</i> .....	39

1.3.5. Riesgos de los dispositivos informáticos .....	41
1.3.6. Casos de noticias. La Blue Whale.....	42
1.4. El primer paso: <i>on line safety</i> .....	44

## CAPÍTULO II

### Intervenciones políticas y sociales para el desarrollo de habilidades digitales

2.1. Iniciativas en Europa .....	48
2.2. Iniciativas en Italia .....	64
2.3. Entrenamiento de seguridad en línea .....	67
2.3.1. Desafíos en línea	
2.3.2. Decálogo para educadores	
2.4. Legislación nacional y europea .....	75
2.5. <i>Safer Internet Day</i> .....	77

## SEGUNDA PARTE

### MÉTODO, RESULTADOS Y CONCLUSIONES

## CAPÍTULO III

### Claves del entorno digital

3.1. Los sistemas de información para la escuela. Un ejemplo de un sistema de gestión escolar .....	82
3.2. Procedimientos de seguridad.....	83
3.2.1. Entrevista con el Vicepresidente de Argo Software .....	84
3.2.2. Entrevista con el Dr. Giovanni Gianni.....	89

3.2.3. Entrevista con el asistente técnico del laboratorio (AT) .....	92
---	----

## **CAPÍTULO IV**

### **Análisis del contexto escolar**

4.1. Ciclo de la escuela italiana .....	98
4.2. Escuelas privadas laicas .....	102
4.1.1. Subvenciones y desgravaciones fiscales para las escuelas privadas .....	103
4.1.2. Contexto económico y social en la ciudad de Victoria .....	107
4.1.2. El instituto público .....	111
4.1.3. El instituto concertado.....	114

## **CAPÍTULO V**

### **Diseño metodológico del estudio de campo**

5.1. Estrategias de aplicación de los instrumentos .....	118
5.1.1. Tratamiento de datos .....	124
5.1.2. Las etapas de la investigación .....	136
5.1.3. La muestra .....	136
5.1.4. Los criterios de evaluación.....	137
5.1.5. Instrumentos y validación del cuestionario .....	138
5.1.6. Procedimiento .....	140
5.1.7. El cuestionario.....	141

## **CAPÍTULO VI**

### **Exposición y comentario de resultados**

6.1. Comparación de resultados según la tipología de centro .....	146
6.1.1. Análisis de los resultados del Instituto Escolar público.....	146
6.1.2. Análisis de los resultados de la escuela concertada .....	164
6.1.3. Comparación de resultados entre centros públicos y concertados .....	189
6.1.4 El papel de los profesores y los padres .....	193
6.1.5. Triangulación de la evaluación .....	195

## **CAPÍTULO VII**

### **Conclusiones generales**

7.1. Consideraciones finales.....	198
7.2. Propuesta .....	203

## **REFERENCIAS**

<b>Referencias Bibliográficas</b> .....	204
<b>Webgrafia</b> .....	214

## **ANEXOS**

<b>CUESTIONARIOS</b> .....	218
----------------------------	-----



## Índice de tablas

NÚMERO	TÍTULO	PÁGINA
Tabla 1:	Resumen de propuestas europeas sobre competencia digital	50
Tabla 2:	Resumen de los proyectos digitales para una nueva didáctica en la red.	59
Tabla 3:	Lista de los recursos más utilizados internacionalmente	70
<b>Tabla 3</b>	Resumen de los valores que faltan en el registro de los padres de los alumnos del instituto estatal "X"	126
Tabla 4	Resumen de los valores perdidos en el registro de los profesores de los alumnos del instituto público "X"	127
Tabla 5	Resumen de valores faltantes en la distribución de registros de los estudiantes de la escuela integral estatal "X "	128
Tabla 6	Resumen de los valores que faltan en el registro de los padres de los alumnos del Instituto privado..	130
Tabla 7	Resumen de los valores faltantes en el registro de los profesores de los alumnos del Instituto privado.	131
Tabla 8	Resumen. Faltan valores en el registro de los alumnos del Instituto privado.	132
Tabla 9	Distribución de frecuencias de los modos de respuesta a la pregunta sobre la libertad en el aula de usar el teléfono móvil	148
Tabla 10	Número de horas/día pasadas frente a la PC, la tableta y el teléfono móvil	151
Tabla 11	La mejor manera de usar las redes sociales	154
Tabla 12	La definición de las tres R de residuos	156

Tabla 13	La opción menos útil para la gestión de los desechos	157
Tabla 14	Burlarse de los defectos de alguien en su blog	160
Tabla 15	¿Qué problemas plantea la inclusión de audio, vídeo y fotografías personales en los sitios web?	161
Tabla 16	Invitación por correo electrónico a una fiesta a una dirección desconocida	161
Tabla 17	¿Qué consejo le daría a su abuelo que recibe un correo electrónico con el logo del Banco donde depositó sus ahorros, que contiene la solicitud de códigos de acceso y contraseñas?	162
Tabla 18	Distribución por sexo de los profesores del instituto técnico-comercial del igual número de profesores	165
Tabla 19	La opinión de los profesores sobre la libertad de los alumnos de usar teléfonos móviles en el aula	166
Tabla 20	La opinión de los profesores sobre lo bien informados que están los jóvenes sobre los programas de seguridad	166
Tabla 21	La distribución sobre la práctica de conductas dirigidas a salvaguardar los datos personales responde a los profesores	168
Tabla 22	Posibilidad de utilizar los teléfonos móviles en el aula según la opinión de los padres de la institución paritaria	169
Tabla 23	Distribución de los modos de respuesta para hombres y mujeres	172
Tabla 24	Número de horas/día pasadas frente a la PC, la tableta y el teléfono móvil	174
Tabla 25	El acoso cibernético puede ocurrir a través de computadoras, teléfonos móviles y tabletas	178
Tabla 26	Conocimiento de las estrategias de protección	179
Tabla 27	Protección del medio ambiente	180

Tabla 28	Definición de desechos electrónicos	181
Tabla 29	La opción menos útil para la gestión de desechos	182
Tabla 30	Cuando se trabaja en un escritorio, la cabeza y el cuello deben estar alineados con el torso	183
Tabla 31	Pago en línea de una entrada para un concierto	185
Tabla 32	En qué sitio introducir sus datos personales	186
Tabla 33	¿Qué problemas plantea la inclusión de audio, vídeo y fotografías personales en los sitios web?	187
Tabla 34	Relación entre las respuestas y la edad de los estudiantes	192
Tabla 35	Comparación de las respuestas de los distintos agentes	195



## **Abstract**

Safety in the digital environment is an issue of urgent relevance in schools. The fear that pupils can put their personal data at risk, the technological devices given to them in use, their physical and psychological well-being and in some ways the environment, has always been a deterrent, which has limited the use of technology information in educational practices. Today, however, it is no longer possible to keep media away from educational practice or teaching design, while recognizing the risks to which one exposes oneself to being subjected to the fascination in an uncritical and indiscriminate way. The acquisition of digital skills related to safety represents, as a consequence, an obligatory passage in the information society and education. This contribution presents data and considerations that emerged following a survey conducted in secondary school. The survey focuses on the concept of online security, according to the model developed by Antonio Calvani.

**Keywords:** on line safety, education, high school, media education, competence analysis

## **Resumen**

La seguridad en el entorno digital es un tema de actualidad en las escuelas. El temor de que los alumnos puedan poner en peligro sus datos personales, los dispositivos tecnológicos que utilizan, su bienestar físico y psicológico y, en cierto modo, el medio ambiente, siempre ha sido un elemento disuasorio, que ha limitado el uso de la tecnología de la información en las prácticas educativas. Sin embargo, hoy en día ya no es posible mantener a los medios de comunicación alejados de la práctica educativa o de la planificación educativa, aunque reconocemos los riesgos a los que nos exponemos al sufrir su fascinación de forma acrítica e indiscriminada. La adquisición de conocimientos digitales relacionados con la seguridad representa, por consiguiente, un paso obligado hacia la sociedad de la información y la educación. En este documento se presentan los datos y consideraciones que surgieron de una encuesta realizada en la escuela secundaria. La encuesta centra su atención en el concepto de seguridad en línea, según el modelo desarrollado por Antonio Calvani.

**Palabras clave:** seguridad on-line, educación, educación secundaria, educación media, competencia digital.

*En este dejar y tomar, huir y buscar,  
realmente parece ver una mayor determinación:  
que a tales seres se les da una especie de voluntad y una capacidad de elección,  
y encuentras un término técnico como  
afinidades electivas.*

GOETHE

## INTRODUCCIÓN

### **1. El proyecto: la seguridad en línea**

El conjunto de cuestiones relativas a la seguridad en línea constituyen temas muy controvertidos en los ámbitos escolares (Jenkins, 2010). De hecho, existe el temor constante de que los alumnos mediante los dispositivos tecnológicos que utilizan, pongan en peligro sus datos personales, su bienestar físico y psicológico y, en cierto modo, también el entorno que nos rodea. Estos temores siempre han sido un elemento disuasorio que ha limitado el uso de la tecnología de la información en las prácticas educativas (Calvani, Fini y Ranieri, 2010).

Sin embargo, hoy en día ya no es posible mantener los nuevos medios de comunicación de masas (sitios, blogs de redes sociales y todos los dispositivos sociotécnicos de difusión

mundial) alejados de las prácticas educativas y de la planificación didáctica. A pesar del reconocimiento de los riesgos a los que, en general, los estudiantes se exponen al experimentar la fascinación de forma acrítica e indiscriminada.

La tecnología de la información, la radiodifusión generalizada y el uso de recursos de red han entrado de manera abrumadora en la vida social de todos los países industrializados, ofreciendo un acceso sin precedentes a los recursos culturales del mundo y promoviendo la participación masiva en los procesos políticos, culturales y sociales del mundo moderno.

De modo que la adquisición de conocimientos sobre los entornos digitales y las habilidades de uso, resultan, por lo tanto, condición necesaria en la actual sociedad de la información y de la educación.

Consideramos que en la base de este proceso de adquisición ha de estar el dominio de la seguridad en línea. Los movimientos en esta dirección parten, de manera decisiva, precisamente de las nuevas políticas europeas, que se detallarán en los capítulos siguientes. La intención explícita de estas políticas parece ser preparar a los jóvenes para aprovechar las ventajas y evitar los riesgos de la tecnología digital.

El primer objetivo de estas intervenciones es, de manera decisiva, formar a los jóvenes en la responsabilidad, el sentido cívico, el respeto y la conciencia, tanto en la realidad virtual como en la vida cotidiana.

Este imperativo en las escuelas también concierne a los educadores que, en primer lugar, parecen no ser plenamente conscientes de las ventajas, y a veces no están preparados para los riesgos, a que da lugar el uso indiscriminado de los nuevos medios de comunicación (entendidos como formas de comunicación interactivas e individualizadas como los medios sociales, el correo electrónico, las salas de *chats*, blogs, canales de vídeo, las aplicaciones en teléfonos inteligentes y tabletas... etc.).

A partir de los estudios y la experiencia directa, creemos que abordar la digitalización de las escuelas, con énfasis en la seguridad, es la palanca de motivación para diseñar actividades educativas y procesos de formación para los estudiantes. Acciones educativas que incluyen la promoción de una comprensión crítica de los medios de comunicación y una utilización prudente y discriminada de sus recursos.

Desde los debates políticos hasta las noticias, desde las leyes de la Buena Escuela (Baldacci, Brocca, Frabboni, & Salatin, 2016) hasta las indicaciones ministeriales, las escuelas emergen como protagonistas de este codiciado pero muy temido cambio.

Una institución que, por su posición estratégica, su amplia difusión de información y su carácter explícitamente formativo, representa sin duda el centro neurálgico de esta transformación.

En Italia es el documento sobre la Buena Escuela con la Ley 107/2015, el último y más detallado documento sobre el desafío educativo que el país le plantea al sistema escolar (Baldacci et al., 2016).

En el citado documento legislativo se confía a las instituciones educativas la tarea de transformar el riesgo del uso indiscriminado de los nuevos medios de comunicación en acciones específicas y relevantes desde el punto de vista educativo.

Nuestro trabajo en esta tesis doctoral se centra en una de las ocho competencias clave identificadas por la Comisión Europea en su Recomendación de 2006, (CE. 2006): la competencia digital. Hemos abordado esta competencia, que consideramos prioritaria, desde la perspectiva de la seguridad en línea.

## **2.Propuesta de estudio**

El proyecto, desarrollado por nosotros, parte de la convicción de que en la innovación tecnológica ya en marcha, la dimensión de evaluación y estadística ha sido descuidada o subestimada. Lo que falta es una base de datos nacional de referencia que pueda darnos el valor exacto de la competencia que poseen los estudiantes italianos.

Queríamos investigar el nivel de competencia que poseen los estudiantes que cursan el tercer año de la escuela secundaria (que corresponde, aproximadamente, a 16 años de edad) para reconocer, discriminar y hacer frente a las amenazas cibernéticas.

Impulsados por la certeza de que dejar la tecnología e Internet fuera del aula no impide que los alumnos puedan acceder a ellas desde su casa o desde cualquier otro lugar; convencidos de que la exposición a estas cuestiones, lejos de las figuras expertas sin una formación adecuada



sobre el uso de las tecnologías en línea, representa una verdadera emergencia social. Hemos concebido este estudio que tiene como objetivo:

Identificar el nivel competencia sobre la seguridad en el entorno digital que poseen los estudiantes al finalizar la escolaridad obligatoria italiana.

- Observar el fenómeno desde el punto de vista de los estudiantes, profesores y padres;
- Analizar y comparar los datos de los dos institutos escolares (estatales y concertados) que se están examinando;
- Proponer la creación de una plataforma nacional de evaluación y estadística sobre la competencia de la seguridad en línea. Ser al mismo tiempo un instrumento de diagnóstico y capacitación, siempre actualizado mediante métodos participativos típicos de la nueva cultura en línea.

Encontramos, en el contexto italiano, un modelo de competencia digital creado por Antonio Calvani , desarrollado magistralmente para verificar las habilidades digitales a través de un conjunto de pruebas para estudiantes de secundaria de primer y segundo grado. Cuestionario validado con la experimentación nacional. Sin embargo, esta herramienta, en el único sentido de autoevaluación para los estudiantes, se ha puesto a disposición de las escuelas, en su versión en línea.

Las preguntas del cuestionario que utilizamos, han sido tomadas de las pruebas mencionadas anteriormente en los diferentes tipos desarrollados que son:

1. IDCA (Evaluación de Competencia Digital instantánea): son pruebas fáciles de completar y rápidas de evaluar.
2. DCA (evaluación de la competencia situacional). Proponen situaciones que requieren habilidades de resolución de problemas en situaciones problemáticas reales (Calvani, Fini & Ranieri, 2014).

La referencia a los cuestionarios de Calvani, adoptados por nosotros, se limita exclusivamente a las dimensiones éticas y cognitivas, que incluyen el concepto de seguridad en línea.

Nuestra evaluación, por lo tanto, hará uso de:

- Pruebas relacionadas con el conocimiento de términos específicos, utilizados en el lenguaje de la Tecnología de la Información;
- Evidencia de la resolución de problemas dispuestos para identificar los aspectos dinámicos de la competencia en seguridad informática;
- Evidencia de escenarios cortos relacionados con problemas éticos y relacionales.

El estudio en cuestión limita el campo de investigación a dos Escuelas de Segundo Grado, ambas ubicadas en la provincia de Ragusa, donde se administraron los cuestionarios mencionados.

La investigación tiene por objeto conocer el nivel de competencia, en relación con la seguridad informática, que poseen los estudiantes del tercer curso, y sondear las opiniones, creencias y estereotipos de los adultos, en este caso los padres y los maestros, sobre las aptitudes que poseen, o no, los estudiantes/niños en este tema.

El objetivo de este estudio es evaluar el nivel de competencia en materia de seguridad en línea que poseen los alumnos, de las dos instituciones examinadas, cuando llegan a la edad en que abandonan la enseñanza obligatoria y pueden, por tanto, dejar la escuela e incorporarse al mundo laboral.

La hipótesis del estudio es la ausencia de instrumentos de evaluación compartidos y el retraso de las acciones efectivas dirigidas a la capacitación de todos los actores del sistema escolar. Cabe señalar, en relación con los profesores que, aunque animados a formarse por las políticas del gobierno, se ven obligados a lidiar con el conocimiento del idioma inglés, que no siempre se posee. Esta competencia parece más indispensable que nunca para poder aprovechar los interminables recursos de formación y autoformación propuestos por la red.

El trabajo se ha llevado a cabo en 6 fases, que se enumeran a continuación:

#### **a) Introducción y definición del proyecto**

- Revisión bibliográfica sobre competencia digital y seguridad en línea. Estudio a fondo del marco teórico en el que las principales teorías sobre la seguridad en línea han sido definidas y desarrolladas por destacados académicos e investigadores en la materia;
- Profundización del debate internacional sobre la utilidad de las tecnologías de información en red aplicadas a la didáctica. Riesgos y oportunidades en juego;

- Iniciativas a favor de la cultura de seguridad en línea nacional e internacional;
- Estudio de las normas relativas al tema de la seguridad en línea. Acciones políticas y sociales desarrolladas en Italia y Europa;
- Entrevistas en profundidad. Entrevista con el vicepresidente de la mayor casa italiana de software, creador del software para la gestión de la red de la administración escolar; entrevista con el Dr. G., especialista en medicina física y de rehabilitación, director de salud de un centro especializado de reeducación sanitaria; entrevista con un asistente técnico de laboratorio, figura introducida en los institutos escolares, para el mantenimiento del hardware y el software presentes en los laboratorios de informática y para ayudar a la didáctica en las actividades de laboratorio.

## **b) Metodología**

- Preparación del cuestionario con referencias y validaciones;
- Método aplicado y criterios elegidos para el análisis y la evaluación del resultado;
- Recopilación de datos sobre los niveles de seguridad en línea de los estudiantes que asisten a los institutos examinados;
- Análisis de contexto y comparación entre las dos escuelas examinadas (estatal y concertada);
- Procedimiento;
- Análisis, comparación e interpretación de datos;

## **c) Conclusiones**

- Conclusiones y consideraciones finales;
- Límites del estudio;
- Propuestas finales.

El objetivo final de este trabajo es tener una evaluación de referencia de la competencia en seguridad en línea que poseen los estudiantes, utilizando una batería de preguntas validadas. Gracias a este sistema de evaluación, será posible reproponer la prueba a otras escuelas,

comprender el nivel de competencia relativo a la seguridad en línea que poseen los estudiantes de un área específica (región o país) e intervenir de manera consciente en las lagunas cognitivas de los estudiantes, identificadas por el cuestionario. Las opiniones y evaluaciones de los profesores y los padres serán otros puntos de vista que se evaluarán para comprender el fenómeno.

De una reflexión sobre los datos que surgieron de esta encuesta se desprende que, a pesar del interés suscitado a nivel nacional e internacional por conceptos como el aprendizaje permanente; a pesar de las recomendaciones europeas sobre los cursos de riesgo en la red; a pesar de las numerosas certificaciones en materia de tecnología de la información proporcionadas por organismos privados y estatales, todavía existen profundas lagunas en la formación de los estudiantes italianos. La formación institucionalizada, de hecho, no se ha transformado, en el sentido de un cambio y replanteamiento de los modelos de formación y aprendizaje, como podría haber sido gracias a la digitalización, pero ha seguido estando vinculada a "competencias técnico-procedimentales específicas" (Calvani, et al., 2014).

La competencia digital, necesaria hoy en día, de la que habla Calvani (2014), se refiere a una estructura compleja y matizada que requiere un conocimiento crítico de las tecnologías, la capacidad de rastrear las fuentes y la veracidad de la información recuperada en línea, y una conciencia ética de las acciones actuadas y vividas en línea. En este marco, la investigación educativa debe desarrollar procedimientos educativos que sean a la vez pertinentes y estén vinculados a los objetivos de la educación formal impartida por la Escuela (Calvani et al., 2014).



## **PRIMERA PARTE**

### **FUNDAMENTACIÓN TEÓRICA**



## CAPÍTULO I

### Revisión del estado de la cuestión

Según la literatura internacional más acreditada, la utilidad potencial de la red y las nuevas tecnologías en el ámbito de las ciencias de la educación y la formación se comparte ahora multilateralmente (Biasi, 2017; Calvo, Ciotti, Roncaglia & Zela, 2003; Ferri, 2005). Los entornos virtuales, el aprendizaje inmersivo, la cultura participativa y la tutoría eficaz en línea han contribuido a aumentar la calidad del aprendizaje y los procesos en los entornos de aprendizaje en red. La capacitación en línea tiene el potencial y las herramientas para competir en eficacia y validez con la capacitación presencial (Calvani & Rotta, 2000). Esta declaración va seguida, de manera igualmente incisiva, por la prometedora reflexión de Trentin<sup>1</sup> (2001) que considera que el alcance de los nuevos recursos telemáticos es ilimitado. Este entusiasmo por la digitalización de la didáctica también es compartido plenamente por Prensky<sup>2</sup> (2001) que coloca, sin embargo, como condición primordial, la adquisición de

---

<sup>1</sup> Guglielmo Trentin es investigador en el Istituto Tecnologie Didattiche del CNR en Génova. Se ocupa del uso educativo de los recursos telemáticos.

<sup>2</sup> Marc Prensky es un escritor, consultor e innovador americano en el campo de la educación y el aprendizaje. Se le conoce como el inventor y difusor de los términos digital nativo e "inmigrante digital", que describió en un artículo de 2001 sobre "On the Horizon".



conocimientos y habilidades que integren el bagaje tecnológico que se posee, porque “digital natives” (Prensky, 2001), con habilidades de interacción críticas y responsables. Esas transformaciones darán resultados satisfactorios y tranquilizadores si los profesores recurren a una formación preventiva que se convertirá en aprendizaje a lo largo de toda la vida. Es necesario que el enfoque de la digitalización, por parte de los profesores, implique también para ellos una transformación radical de las metodologías de aprendizaje y de la utilización de los recursos en línea, y no una simple adaptación de los programas de enseñanza tradicionales a las nuevas tecnologías. Hacer didáctica en línea significa transformar el proceso de enseñanza-aprendizaje de manera global (Rossi, 2014). La facilidad con que la inmensa cantidad de información permite la interacción entre las diferentes materias y temas de estudio, es un atractivo esencial para los instructores que pueden elegir entre tutorías, programas informáticos educativos de código abierto, gratuitos, de pago, formación social, actividades de aprendizaje permanente, intercambios culturales entre países y mucho más. Sin embargo, aunque los nuevos medios de comunicación puedan parecer "auto-alfabetos", también son un atractivo para los entrenadores (Rivoltella & Ferrari, 2014), sólo que aparentemente no necesitan mediación educativa. Para gestionarlos de manera segura y responsable, no sólo se necesitan conocimientos y habilidades operacionales, sino también nuevos enfoques culturalmente significativos (Rivoltella & Ferrari, 2014). El papel de los profesores, si en algunas áreas se reduce y se sustituye por la tecnología, sigue siendo, sin embargo, siempre central y decisivo. Especialmente cuando la formación educativa está orientada al aprendizaje crítico y responsable.

## **1.1. Digital Literacy**

La *On line Safety*, a la que nos referimos en nuestro estudio, es uno de los elementos relacionados con la *Digital Literacy* (DL). Comencemos, por lo tanto, con el término DL, que ha sido objeto de teorías controvertidas a lo largo de los años. Ha evolucionado rápidamente y se ha expandido a lo largo de los años, añadiendo siempre nuevas habilidades y significados a su definición inicial. El término DL deriva de la alfabetización digital y se refiere a las aptitudes digitales, como las técnicas y procedimientos necesarios para el desarrollo de nuevas tecnologías. (Calvani, Fini, & Ranieri, 2011). Con la aparición de Internet, las habilidades digitales ya no eran suficientes para manejar la avalancha de información de la World Wide

Web. En consecuencia, el concepto de Alfabetización digital amplía la noción de capacidad integrando el pensamiento crítico y las habilidades de producción colaborativa de conocimiento en su significado (Gilster, 1998). A la definición principal se añaden otras habilidades, como la capacidad de manejar información a través de diferentes medios y de abordarlas según los estilos y rasgos de aprendizaje individuales (Bawden & Robinson, 2002). Muchos investigadores identifican la AD como el resultado de aspectos técnicos, habilidades intelectuales y competencias relacionadas con la ciudadanía responsable (Calvani & Menichetti, 2014).

En algunos aspectos, la definición de Eshet-Alkalai (2004: 93) parece diferente, e incluso ligada a las habilidades técnicas, para lo cual la LD debe definirse a través de 5 habilidades alfabéticas que se concretan en:

1. Capacidad de leer instrucciones de interfaces gráficas: Alfabetización visual fotográfica;
2. Capacidad de utilizar la capacidad de reproducción del ordenador: copiar y pegar, para crear productos originales y creativos;
3. Habilidad en la producción escrita;
4. Creatividad (Reproduction Literacy);
5. Flexibilidad cognitiva.

Es evidente que el concepto de DL es muy complejo y difícil de reducir a una sola dimensión. Para su definición es necesario referirse a la integración de varias dimensiones: habilidades técnicas, cognitivas y metacognitivas, así como conceptos relacionados con la participación cívica y la conciencia ética. En la definición del término (DL) es de particular importancia la explicación que Jenkins<sup>3</sup> da de las nuevas *Media Literacies*. Enfatiza la dimensión social y pública de la alfabetización mediática, comparada con la dimensión subjetiva y aislada. La alfabetización, de hecho, tiene la preciosa peculiaridad de manejar dimensiones diferentes y en constante evolución a través de nuevos canales y herramientas. (Jenkins & Lacasa, 2010). La definición de competencia digital elaborada en el modelo DCA (Digital Competence

Assessment<sup>4</sup>), de la que también partimos como punto de referencia para esta investigación, se define como la capacidad de hacer frente a los nuevos contextos a los que se exponen las nuevas tecnologías de manera flexible, la capacidad de reconocer la fiabilidad de las fuentes y la información, la capacidad de participar activa y conscientemente en un conocimiento participativo (Calvani & Menichetti, 2014). Navegando a través de la literatura en este campo, encontramos otras opciones de terminología que describen las competencias digitales de acuerdo a su campo. Por ejemplo:

- El concepto de *Media Literacy* o *Media Education* se entiende como la adquisición de conocimientos técnicos y prácticos para la recepción analítica y crítica de los mensajes de los medios de comunicación en el ecosistema político, cultural y económico. (Pérez-Tornero, 2004). También los modelos teóricos de la educación sobre los medios de comunicación elaborados por Buckingham (2006), se refieren a la comprensión crítica de los medios de comunicación. Estos, de hecho, se entienden no sólo como herramientas, sino como lenguaje y cultura.
- El término *Information Technology Literacy* define la competencia digital como la capacidad de un individuo para trabajar tanto en equipo como de manera autónoma; para utilizar de manera responsable las herramientas, los recursos, los procesos y los sistemas; para acceder a la información en cualquier medio; para utilizar esa información con capacidad para resolver problemas; para comunicarse correctamente; para tomar decisiones informadas; para crear nuevos conocimientos, productos o sistemas. (McMahon, 2014).
- El término *Information Literacy* define la competencia digital como la capacidad de adquirir y utilizar información de manera adecuada en cualquier situación, tanto a nivel local como mundial; de sobrevivir y tener éxito en un entorno de información y tecnología; de llevar una vida productiva, sana y satisfactoria en una sociedad democrática; de trabajar eficazmente en entornos que cambian rápidamente; de asegurar un futuro mejor para la próxima generación; de encontrar información adecuada para resolver problemas personales (Bawden & Robinson, 2002).

---

<sup>4</sup> Istant Digital Competence Assessment (iDCA) es una herramienta de evaluación de la competencia digital diseñada como parte del Proyecto de Investigación de Interés Nacional. (PRIN MIUR D.M. n. 582/2006 del 24 marzo 2006) da Antonio Calvani.

Esta definición: Information Literacy viene de *Association of College and Research Libraries* (ACRL), que explica cómo la capacidad de comprender las propias necesidades de formación y de evaluar críticamente la información y sus fuentes (American Library Association, 2000).

El concepto de *Visual Literacy* se entiende, en cambio, como la capacidad de leer, interpretar y decodificar imágenes de la misma manera crítica que se utiliza para un texto (Calvani et al., 2010).

- El término *Network Literacy* enfatiza, en cambio, los aspectos sociales de la Digital Literacy (Gapski, 2008; Martin & Grudziecki, 2006; Midoro, 2007; Pérez-Tornero, 2004).

Las múltiples interpretaciones y definiciones de la competencia digital varían, como hemos visto, según el campo al que pertenecen. Hablando del entorno escolar, la noción de competencia digital que más nos interesa se refiere a las modalidades educacionalmente relevantes (Calvani & Menichetti, 2014). Esto implica habilidades y destrezas cognitivas, relacionales y sociales; destrezas de resolución de problemas y metacognición; destrezas inferenciales y deductivas; sensibilidad al contexto sociocultural y a los contextos en uso.

La Comisión Europea, que ha asumido un papel fundamental en el desarrollo de las aptitudes electrónicas, se refiere a la competencia digital como el recurso para un enfoque consciente de la tecnología de la información en todos los ámbitos de la vida: laboral, social y lúdico. El ordenador de hecho, representa el medio más extendido para entrenar, actualizar, comunicar y producir información. (EC, 2006). Esta competencia no se refiere a los conocimientos informáticos que los niños desarrollan de forma independiente y autónoma. (Buckingham, D., Banaji, S., Carr, D., Cranmer, S., & Willett, R. 2005), sino a otro tipo de alfabetización que depende, principalmente, de factores específicos que poseen los jóvenes marineros, entre ellos:

- El nivel general de desarrollo cognitivo, emocional y social;
- La experiencia del mundo en general;
- La experiencia específica de los medios de comunicación.

Según esta teoría, todo intento de promover cualquier forma de alfabetización mediática debe dejar de lado la evaluación de las aptitudes pasadas, en relación con los factores descritos (Buckingham, et al., 2005). La "inundación de información" (Lvy, 1997) de los años noventa y con ello la explosión de Internet y las redes sociales entre los adolescentes, ha desplazado el centro de atención a un aspecto específico de la competencia digital, a saber, el concepto de fiabilidad. Desde 2000, de hecho, el foco de las nuevas investigaciones universitarias se ha centrado en la fiabilidad, la seguridad y la ética (Jenkins et al., 2009). Estos conceptos parecen ser aún más importantes en relación con las nuevas demandas de libertad, las nuevas formas de compartir y socializar dictadas por la cibernavegación. (Himanen, 2003). Nace así un nuevo reto para los profesores que navegan en línea: el de garantizar la seguridad en Internet. Surge la importancia de la Seguridad en línea, entendida como la capacidad de navegar por la red con precaución, consciente de los riesgos pero también de los deberes a cumplir, respetando los derechos propios y los de los demás. En otras palabras, una sociedad multiparticipativa y multimedia en la que "participar de forma éticamente consciente" (Calvani et al., 2014).

## **1.2. Educación y medios de comunicación: "afinidad electiva"**

Educación y Medios de Comunicación son dos conceptos, sólo en apariencia, diametralmente opuestos: uno dirigido al pasado, basado en la razón, la objetividad y que aspira a la formación ética del buen ciudadano. (Jacques, 2001) la otra dirigida a la actualidad, basada en lo efímero, en la subjetividad y condicionada por factores económicos, políticos y sociales. La contribución de Jacques va en la misma dirección que el estudio de Jenkins<sup>5</sup> (Jenkins, Purushotma, Weigel, Clinton, & Robison, 2009). De hecho, sostiene que la educación escolar, en su formalidad, siempre ha demostrado estar encaramada a posiciones tradicionalistas. La adquisición de competencias culturales de manera no tradicional, en cambio, a menudo adquirida de manera autodidacta, se refiere, por necesidad, a una metodología experimental. Lo formal por convención se identifica con algo inmóvil y estacionario; lo informal, en

---

<sup>5</sup> Henry Jenkins es profesor de comunicaciones y periodismo en la Universidad del Sur de California. Fue codirector del Programa de Estudios de Medios Comparados del MIT en Boston. Creó el "Laboratorio de cultura participativa y aprendizaje" en Los Ángeles. Es autor y editor de muchos libros sobre diferentes aspectos de los medios de comunicación y la cultura popular, incluyendo "Convergencia de la cultura" (Apogeo 2008) que ahora se considera un clásico en todo el mundo.

cambio, parece estar vinculado al aprendizaje libre y libre de las reglas tradicionales, y por esta razón parece más inclinado a aceptar metodologías innovadoras. Las nuevas metodologías de aprendizaje apoyadas por las tecnologías multimedia son capaces de responder a necesidades transitorias y variables. Por otra parte, las instituciones de enseñanza formal parecen estar empantanadas durante decenios en procedimientos complejos y engorrosos, a pesar de las numerosas reformas que se les han aplicado. El sistema de educación formal reproduce una trayectoria de aprendizaje preestablecida y estacionaria, refractaria, en la práctica, a todo esfuerzo de cambio y a toda posibilidad de elección o movilidad. El sistema de aprendizaje informal, por otra parte, permite experimentar esa movilidad. (Jenkins, Purushotma, Weigel, Clinton, & Robison, 2009). De hecho, en algún momento de la historia los medios y la educación comenzaron a encontrarse e influenciarse mutuamente. Por un lado, la Escuela tomó conciencia de la omnipresencia de los medios de comunicación en todos los ámbitos de la sociedad, por otro lado el sistema de medios de comunicación comenzó a cuestionar su papel en la sociedad y en el campo de la educación. (Giannatelli, 2001). La colaboración entre los medios de comunicación y la educación reglada, en nuestra opinión, es el entorno propicio para el desarrollo de la educación y la institución educativa por excelencia. Y es en el ámbito escolar en el que las dos realidades: Medios y Educación,

...dan lugar a un nuevo compuesto, como una afinidad electiva, los dos elementos unidos por nacimiento o casualidad a otros elementos, se disocian de éstos para unirse y formar una nueva amalgama mucho más resistente que las anteriores. (Goethe, 2011).

La Escuela reconoce que las nuevas tecnologías se contaminan y se integran en formas constantemente diferentes, y cada vez reinventan al individuo, su forma de pensar, de cognitivizar, de actuar en función de objetivos específicos. Esto, a la luz de los nuevos conocimientos, puede preparar, en el entorno escolar, el medio ambiente natural para que los dos procesos de Educación, formalmente entendida, y la información multimedia, se encuentren y enriquezcan mutuamente. Todo esto, sin embargo, debe tener lugar con la conciencia de los riesgos a los que se exponen las herramientas multimedia y, sobre todo, el dispositivo en línea. De hecho, se pide a los educadores y profesores que formen y preparen instrumentos para salvaguardar la seguridad de los estudiantes en lo que respecta a la salud

física y psicológica y a sus datos personales. Para preservar, además, el medio ambiente y los dispositivos que utilizan. Numerosas propuestas a nivel nacional e internacional han abordado el problema de la seguridad en línea. De particular relevancia son las propuestas europeas, que instan a los Estados Miembros a establecer procedimientos para desarrollar nuevas formas de competencia para enseñar a los estudiantes la capacidad de aprender de forma independiente y responsable. Una formación que va más allá del aula y dura en el tiempo, acompañando a los nuevos ciberciudadanos durante toda su vida, actualizando constantemente sus conocimientos y reformulando los métodos de aprendizaje a la luz de las exigencias siempre cambiantes de la vida y el trabajo (Jenkins, 2010). Sin embargo, en la actualidad, creemos que no podemos prescindir de las instituciones de formación en este proceso de aprendizaje. En cambio, esperamos una reforma radical del sistema educativo. Una reforma que no es un mero compromiso entre la cultura clásica y los modelos participativos, sino una afinidad electiva. Se trata, como afirman Alberto Marinelli y Paolo Ferri en la introducción a *Culturas Participativas y Competencias Digitales*, de dar confianza a las nuevas formas de conocimiento que ofrece la red e integrarlas en la práctica escolar. Modos de aprendizaje que ya están en posesión de los jóvenes nacidos, culturalmente en entornos digitales (Jenkins, 2010). La Escuela es, por su naturaleza, el lugar ideal para este encuentro entre la cultura y los estilos de aprendizaje participativos, típicos de la red. Una reunión en la que se conservan los conocimientos y contenidos tradicionales y en la que se renuevan los métodos y estilos de aprendizaje. El primer paso en esta dirección, pensamos, es la formación de la conciencia y la conciencia social, por parte de las instituciones educativas y las familias.

### **1.3. Riesgos y beneficios de la sociedad de la información**

El nacimiento de los llamados "nativos digitales" (Prensky, 2001), para el que los medios de comunicación han desempeñado un papel fundamental, ha puesto en primer plano el debate sobre la seguridad mundial. A través de los nuevos medios de comunicación, las generaciones 2.0 han llegado a los canales de comunicación, considerados "libres". En estas áreas virtuales los usuarios desarrollan y mantienen amistades, viven y comparten su intimidad en una especie de "diario" virtual. Las redes sociales se han convertido en el lugar donde se comparten los intereses, pero también en el conjunto donde se construye y define la identidad. Casi todas las actividades a las que uno se dedica están conectadas, de una forma u otra, con

la navegación online. Van Deursen (2010) identifica al menos 5 áreas en las que el uso de Internet es beneficioso para los ciudadanos (social, económico, sanitario, político y cultural). Esboza los principales aspectos de estas áreas:

1. Representa un beneficio social, al ofrecer la posibilidad de intercambiar conocimientos y de entrar en contacto con comunidades que comparten los mismos intereses, a pesar de la diferente ubicación geográfica de los miembros. La Internet fomenta la integración entre los pueblos, asegura la comunicación, proporciona las herramientas para la participación cívica y política, desarrollando sentimientos de inclusión y realización;
2. Representa un beneficio económico cuando permite a las personas encontrar trabajos más rentables y satisfactorios, beneficiándose de la amplia oferta que ofrece Internet. La información, de hecho, a la que se llega a través de la red puede convertirse en riqueza cuando le da la oportunidad de ahorrar dinero aprovechando y evaluando más oportunidades que los que no recurren a la red;
3. Representa un beneficio para la salud, cuando mejora la calidad de vida y la autorrealización, gracias a la posibilidad de sentirse parte de un grupo específico. Por ejemplo, a través de las comunidades sociales y en línea, las personas enfermas y sus familias pueden recibir apoyo para enfermedades o problemas específicos, incluso de especialistas en la materia;
4. Es un beneficio político cuando proporciona información actualizada de todo el mundo y de diferentes fuentes. Los ciudadanos más competentes también pueden establecer plataformas para compartir ideas de política o abogar por causas internacionales;
5. Representa un beneficio cultural cuando, a través de la socialización, permite a la gente conocer las costumbres y hábitos de los grupos culturales, sociales o étnicos (Helsper, EJ, Van Deursen, A. & Eynon, R., 2015).

Sin embargo, los resultados de tantos beneficios deben ponerse siempre en contexto (van Deursen, Van Dijk & Helsper, 2014). De hecho, muchas variables complejas podrían intervenir en el proceso de lograr un determinado beneficio. Diferentes son, por ejemplo, los niveles de competencia digital que necesita cada categoría de usuarios. Hay diferentes niveles de digitalización de cada escuela en todo el mundo. La falta de competencia digital, por



ejemplo, afecta negativamente a la misma motivación para utilizar los recursos y herramientas de la red. El ritmo y la omnipresencia de la revolución digital ha ampliado el horizonte de los procesos de la adolescencia, creando una nueva perspectiva de inmersión en el mundo virtual. Este fenómeno debe ser tenido en cuenta, comprendido y apoyado por los adultos. Esta nueva forma de vivir y actuar socialmente es completamente desconocida para las generaciones anteriores. Los padres y los maestros ya no son capaces de cumplir su papel de líderes para las nuevas generaciones. No tienen las habilidades para entrenar o proteger a sus hijos/estudiantes de los riesgos de la red. De algunas entrevistas, realizadas por esta investigación, se desprende una extrema desconfianza, hacia la red, por parte de padres y profesores, que dicen preferir que las prácticas de enseñanza sean ajenas a tales métodos y estilos de aprendizaje. Hay adultos que consideran que la navegación es igual que un videojuego, cuando no consideran que es una exposición arriesgada a los males oscuros. La brecha entre generaciones parece, en muchos sentidos, insalvable hoy en día. La cuestión se refiere a una amplia gama de cuestiones y expectativas, desde las oportunidades percibidas como el aprendizaje en línea, el compromiso cívico, hasta los tan temidos riesgos de la adicción a Internet o la pérdida de privacidad. La conciencia del potencial de Internet es una realidad universalmente reconocida. Pero al mismo tiempo, también lo son los riesgos y temores mencionados en la literatura. Un sólido conjunto de estudios revela, de hecho, la complejidad y la multiplicidad de los riesgos que conlleva la navegación en línea (Jenkins, 2010; Livingstone et al., 2005; Livingstone et al., 2012; Mascheroni, 2012; Ozenda e Bissolotti, 2012; Sonck et al., 2011). El fenómeno se extiende inconmensurablemente si tenemos en cuenta las horas que los jóvenes pasan en la web y cómo están involucrados en ella. Jenkins (2006), partidario de las culturas participativas, nos habla de lugares virtuales donde los jóvenes pueden expresar libremente sus pensamientos, su creatividad, su compromiso cívico. Casi todos los estudiantes, añade, ya han creado y compartido contenidos multimedia al participar directamente en la creación de estos lugares.

Sin embargo, hace hincapié en tres riesgos que llama la atención de los educadores:

1. Desigualdad en el acceso a los recursos;
2. El problema de la transparencia en la transmisión de información por los medios de comunicación;

3. El desafío ético de una educación que debe preparar a los ciudadanos del futuro para participar cada vez más en la vida política y social en un entorno social en línea complejo y diverso (Jenkins 2006).

Compartimos el pensamiento de Jenkins y sus dudas sobre si los jóvenes pueden desarrollar de forma automática e independiente las habilidades necesarias para tratar estos temas. Así como otros estudiosos (Ala-Mutka, K., Punie, Y. & Redecker, C., 2008) que consideran de fundamental importancia la mediación de instructores experimentados en el proceso de alfabetización informática. Las áreas a salvaguardar, subrayan, se refieren a cuestiones como: seguridad, privacidad, participación ética y legalidad; (Ala-Mutka, K. et al., 2008). Sonia Livingstone (2011) hace un análisis aún más detallado de los riesgos a los que se exponen los adolescentes en línea. Indica como principales peligros: la pornografía, el acoso, el sexting, las reuniones con contactos conocidos en línea, la exposición a contenidos nocivos (incitación al odio, anorexia, suicidio, consumo de drogas). A éstos se añaden los riesgos relacionados con la privacidad y la seguridad de los datos y los dispositivos. La reflexión sobre los numerosos trabajos de la literatura en este campo nos ha llevado a identificar los riesgos más comunes para las nuevas generaciones. Son: noticias falsas, robo de datos, ciberacoso, sexting.

### **1.3.1. Fake news**

Las noticias falsas han llenado recientemente las primeras páginas de los medios de comunicación internacionales. Como siempre lo han hecho los antiguos canales de noticias (periódicos, radio o televisión), los medios digitales también ofrecen una versión filtrada de la verdad. Como los primeros, de hecho, no se limitan a presentar la realidad, sino que la interpretan, la endulzan, la modifican y, cada vez más, la manipulan en relación con intereses específicos. Incluso cuando, perfectamente de buena fe, nos informan de las noticias o exponen un punto de vista, el suyo. Los educadores y los expertos en la materia han emprendido varios proyectos a nivel internacional para ayudar a los lectores en línea que están un poco menos preparados. Por ejemplo, para que se reconozca la noticia falsa, el

educador de medios Frank Baker ha compilado una lista de recomendaciones<sup>6</sup> prácticas para los usuarios en línea (Baker, 2017). En la misma línea, el *News Literacy Project* que proporciona una lista de control con diez preguntas para evaluar el grado de fiabilidad de cada noticia<sup>7</sup>. También en los Estados Unidos, la cuestión de la seguridad en línea se trata como un asunto importante. The News Literacy Project (PNL), Por ejemplo, una organización nacional sin fines de lucro, con sede en Washington, DC, trabaja con educadores y periodistas para proporcionar a los estudiantes de secundaria y preparatoria las herramientas para distinguir los hechos de la ficción en la era digital. La PNL proporciona a estos estudiantes las habilidades necesarias para convertirse en consumidores de noticias inteligentes, dándoles la oportunidad de convertirse en ciudadanos informados y participativos en la vida social. Se anima a los estudiantes a compartir y producir información precisa, correcta y responsable que fortalezca sus voces. Cualquiera puede ser editor y, al mismo tiempo, todos deben serlo. El objetivo de la PNL es ver la alfabetización de noticias incrustada en la experiencia educativa americana como una habilidad esencial del siglo XXI. Un sabio artículo de Valerie Strauss<sup>8</sup>, un escritor en el blog Answer Sheet, habla sobre la fundación del News Literacy Project por Alan Miller, periodista y ganador del Premio Pulitzer. A través del proyecto, se propuso educar a los jóvenes para que reconocieran la información falsa recuperada en línea.<sup>9</sup> News Literacy Project está creciendo, dice el Dr. Strauss, como nunca antes en el país, con los profesores buscando recursos para sus estudiantes para ayudarles a evaluar la credibilidad de la información. El sitio ofrece un decálogo de preguntas y respuestas, preparado por Strauss y Miller, que explica por qué comenzó a trabajar en la seguridad en línea, cómo funciona su trabajo y cómo el clima político ha influido en el Proyecto de Alfabetización. Los estudiantes de hoy, añade Miller, deben navegar por el paisaje informativo más desafiante de la historia de la humanidad. Reciben gran parte de sus noticias a través de los medios sociales, donde la información basada en hechos compite con publicaciones, tweets, vídeos, fotos y gráficos que están diseñados para persuadir, vender, explotar, incitar o desinformar. Al igual que el resto de la población, los adolescentes generalmente luchan por diferenciar la información creíble sobre los acontecimientos de la información en bruto, la información errónea y las menciones

---

<sup>6</sup> <https://www.wnyc.org/story/breaking-news-consumers-handbook-pdf/>

<sup>7</sup> [https://www.washingtonpost.com/news/answer-sheet/wp/2018/03/27/not-sure-whats-real-or-fake-anymore-the-news-literacy-project-teaches-kids-how-to-tell-the-difference-and-its-growing-faster-than-ever/?noredirect=on&utm\\_term=.aa6c6d35c77b](https://www.washingtonpost.com/news/answer-sheet/wp/2018/03/27/not-sure-whats-real-or-fake-anymore-the-news-literacy-project-teaches-kids-how-to-tell-the-difference-and-its-growing-faster-than-ever/?noredirect=on&utm_term=.aa6c6d35c77b)

<sup>8</sup> Valerie Strauss e una reporter che copre istruzione, affari esteri Washington DC.

<sup>9</sup> Tratto da <https://www.mercurynews.com/2018/03/27/news-literacy-project-tackles-fake-news-and-business-is-booming/>

falsas. Los investigadores del Grupo de Educación Histórica de Stanford concluyeron en un informe de 2016 que evaluó las habilidades de lectura y escritura de unos 8.000 estudiantes de la escuela media y secundaria, que los estudiantes eran "fácilmente engañados" y mal equipados para navegar con éxito a través de imágenes e información en línea<sup>10</sup>. A la misma conclusión llega David Buckingham, quien ofrece, además de un análisis crítico del problema de las falsas noticias, una serie de ejemplos interesantes (y a veces divertidos) de falsas noticias (Buckingham, 2005). El autor espera que los estudiantes, que pasan cada vez más horas en línea, miren más allá de una URL. org y se pregunten quién está detrás de un sitio. Buckingham añade que, en todos los niveles culturales, se sorprendieron por la falta de preparación de los estudiantes. Las noticias falsas también están en Wikipedia. El erudito cita, como ejemplo emblemático, la parodia del líder norcoreano Kim Jong Un que es votado como el hombre más sexy del mundo. La historia se publicó en el sitio web satírico estadounidense The Onion en 2012, pero fue retomada por el diario oficial China People's Daily, que contenía una colección de fotos de 55 páginas en su sitio web<sup>11</sup>. La noticia burlesca que describe a un hombre bastante normal, como uno de los hombres más bellos del mundo, ha sido difundida y considerada cierta por millones de lectores. Nosotros también creemos que la comprobación de hechos en línea es más importante que nunca hoy en día. Otras acciones a favor del reconocimiento de noticias falsas provienen de muchas partes de Europa. Por ejemplo, el verificador de hechos sueco Viralgranskaren y la Fundación Internet en Suecia (IIS) han publicado la guía de verificación de hechos en línea (la guía está en sueco, pero hay un video en inglés disponible) . La BBC también ha lanzado un plan para ayudar a los estudiantes a identificar las noticias falsas. El canal de televisión también se ha ofrecido a apoyar a las escuelas para ayudar a los estudiantes a reconocer las noticias en línea. La Comisión Europea, que durante años ha sido sensible a las cuestiones relacionadas con las noticias falsas, ha creado un grupo de expertos de alto nivel para abordar el problema de las noticias falsas y la información errónea que difunden<sup>12</sup>. En la acción participan personalidades de los medios sociales, expertos en medios de comunicación y académicos de toda la UE. El grupo está trabajando en el desarrollo de una estrategia, a nivel europeo, para abordar el espinoso problema de las noticias falsas. Damian Tambini, autor de Fake News: Public Policy Responses, señala que la dificultad para erradicar la difusión de noticias falsas se remonta a la

---

<sup>10</sup>Tratto da <https://ed.stanford.edu/news/stanford-researchers-find-students-have-trouble-judging-credibility-information-online>

<sup>11</sup> <https://davidbuckingham.net/2017/01/12/fake-news-is-media-literacy-the-answer>

<sup>12</sup> <https://www.ilpost.it/2018/12/11/il-piano-dellunione-europea-contro-le-fake-news-fa-acqua/>

legalidad de las mismas. Las noticias falsas se han incluido en el concepto de protección de la libertad de expresión (Tambini, 2017). También en este punto, la Comisión Europea ha demostrado ser proactiva y, de hecho, ha puesto en marcha una consulta pública con el fin de recoger las opiniones de una amplia gama de interesados en el fenómeno de las noticias falsas para idear soluciones y proponerlas a la comunidad. La posibilidad de enviar reflexiones y contribuciones sigue abierta.

### **1.3.2. Robo de datos**

La red, incluso antes que las instituciones oficiales, ha creado y difundido numerosos decálogos y conocimientos para los navegadores inexpertos. Los consejos, sugerencias y condiciones de uso inundan el espacio virtual con advertencias más o menos alarmantes y bien fundadas. Sin embargo, a menudo éstos permanecen sin leer o sin escuchar por parte de usuarios distraídos, que detrás de una navegación ahora rutinaria, que tiene lugar en la familiaridad de su propio hogar, no advierten del peligro que se esconde en la red y enlazan de un sitio a otro con una mirada acrítica y superficial. El primer error, indican los expertos, es subestimar, no reconocer la amenaza (como la primera pregunta en el área relacionada con la protección de datos personales en el cuestionario administrado a los estudiantes). De hecho, hay muchas páginas web engañosas y correos electrónicos fraudulentos, que están estructurados para defraudar al usuario e inducirlo a dar detalles sobre sí mismo, a revelar su nombre de usuario y contraseña, o incluso a pagar sumas de dinero a oficinas bancarias o vendedores fantasmas. Ejemplos, estos, cubiertos en la novena pregunta del área de protección de datos personales y en el primer estudio de caso). A menudo se trata de versiones modernas de viejas estafas, difundidas por Internet, con la esperanza de engañar a un número enorme de personas.

Otro peligro muy común al que uno se expone usando Internet es el uso ingenuo de hipervínculos, enlaces vía imagen, video, o incluso aquellos que se activan cuando uno simplemente pasa el ratón por encima de ellos. Al hacer clic en estos enlaces se puede acceder a otra sección de la página web o a otro documento, se puede descargar un programa o archivo, ejecutar un código o enviar un correo electrónico, todo ello sin el conocimiento del usuario. Puede que nos encontremos en un sitio poco fiable o que hayamos descargado involuntariamente malware o un virus (Sammons & Cross, 2017). Estos son algunos de los

contenidos del Cuestionario para Estudiantes, relacionados con el área de protección de equipos informáticos. Pero los mayores riesgos a los que puede estar expuesto no son los relacionados con el apoyo técnico, sino, en nuestra opinión, los relacionados con los datos y la información personal que, a menudo, se comparten profusa e imprudentemente en la red. Al utilizar Internet, debería tomarse un tiempo para pensar en el nivel de privacidad garantizado por los diferentes sitios en los que navegamos; pregúntese cómo se utilizará la información que publicamos en línea, quién podrá verla y cuánto de lo que publicamos permanecerá almacenado. La mayoría de las veces las políticas de privacidad están claramente descritas en los sitios, pero no se leen. A menudo, en las páginas web que visitamos hay enlaces a "Condiciones de uso", a políticas de privacidad que, si se leen, podrían informarnos sobre los criterios para compartir con terceros, el famoso consentimiento informado (Sammons & Cross, 2017). Como nos advierte el Garante de la Privacidad, estamos distribuyendo cada vez más nuestros datos a cambio de servicios en línea "gratuitos". Un lema, cínico pero veraz, que circula en la web dice: "si no pagas por el producto, el producto eres tú". Este aforismo se aplica particularmente bien a todos los servicios gratuitos que se ofrecen en la Web: motores de búsqueda, alojamiento de su blog, servicio de correo electrónico, redes sociales y todas las aplicaciones. Desde el punto de vista de la alfabetización mediática, esto significa que los alumnos deben aprender, entre otras cosas, a reconocer cómo se generan los beneficios de las aplicaciones gratuitas y cuáles son los intereses comerciales subyacentes. Un informe reciente, *Growing Up Digital*,<sup>13</sup> de digital taskforce Growing Up El Reino Unido, destaca la dificultad de los adolescentes y otras personas para identificar sus derechos en relación con las empresas de medios de comunicación social. El informe describe cómo los términos y condiciones de Instagram, por ejemplo, abarcan 17 páginas y 5.000 palabras, con estructuras lingüísticas y sintácticas difíciles de entender. Como seguimiento a este ejercicio, el Comisionado de la Infancia pidió al bufete de abogados Schillings que desarrollara versiones simplificadas de los Términos y Condiciones para Instagram, Facebook, Snapchat, YouTube e WhatsApp<sup>14</sup>. Mientras que antes el tema de la seguridad en línea era un asunto exclusivo de los especialistas en informática o de las grandes empresas, ahora es una preocupación que no excluye a nadie. El problema afecta a los responsables de las empresas o instituciones, pero también al simple operador que accede a los sistemas informáticos o los utiliza. La amenaza también se ha vuelto extremadamente grave debido al aumento del número de agentes

---

<sup>13</sup> <https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/>

<sup>14</sup> <https://www.tes.com/teaching-resources/digital-citizenship>

criminales que actúan en línea. A lo largo de los años, los miembros de la red de Insafe, la asociación europea de referencia para un mejor uso de la Internet y una navegación más segura, han creado múltiples recursos de alfabetización en los medios de comunicación, a menudo combinados con actividades y campañas más amplias. En Austria, por ejemplo, el Ministerio de Educación ha aplicado una estrategia para el desarrollo de las aptitudes digitales. El proyecto llamado "digi.komp"<sup>15</sup>, está dirigido a jóvenes de entre 6 y 14 años de edad. Austrian Safer Internet Center<sup>16</sup> asociación ya presente en la red antes de las acciones promovidas por el Ministerio, la ha apoyado de diversas maneras, proporcionando manuales y cursos de formación para profesores. Además de la red Insafe, a la que nos referimos a menudo, hay muchos ejemplos de recursos y actividades que pueden inspirar a los profesores a enseñar sobre la protección de datos y la privacidad:

- *European Handbook for Teaching Privacy and Data Protection at Schools*<sup>17</sup> El manual europeo para la enseñanza de la privacidad y la protección de datos en las escuelas. Basado en el proyecto ARCADES, disponible en inglés, húngaro, polaco y esloveno.
- *Digital Defenders vs. Data Intruders – Privacy for kids!*<sup>18</sup> Una guía para aquellos que quieren defenderse digitalmente contra los intrusos de datos, también adecuada para los niños. Para ayudar a los jóvenes de 10 a 14 años a proteger su privacidad.
- *Helping schools*<sup>19</sup>. Un kit de auto-revisión de Safer Internet Center en el Reino Unido para ayudar a las escuelas a cumplir con la protección de datos.
- *That data, actually OUR data, in the Cloud*. Estos datos, en realidad NUESTROS datos, provienen de la Luxembourg Safer Internet Center<sup>20</sup>.
- *Guide to Online Services on the Better Internet for Kids (BIK) website*<sup>21</sup>. La Guía de servicios en línea del sitio web Better Internet for Kids (BIK), que ofrece información clave y directrices detalladas en varios idiomas sobre aplicaciones populares, sitios de redes sociales y otras plataformas utilizadas comúnmente por niños, jóvenes y adultos.

---

<sup>15</sup> <https://www.digikomp.at/>

<sup>16</sup> <https://www.betterinternetforkids.eu/web/austria/profile>

<sup>17</sup> <https://vublsts.wordpress.com/2016/07/29/the-european-handbook-for-teaching-privacy-and-data-protection-at-schools/>

<sup>18</sup> <https://edri.org/papers/privacy-for-kids/>

<sup>19</sup> <http://communityhelpingschools.org/>

<sup>20</sup> <https://www.betterinternetforkids.eu/web/luxembourg/profile>

<sup>21</sup> <https://www.betterinternetforkids.eu/hu/web/portal/>

En Finlandia, la Semana de la Alfabetización en los Medios de Comunicación se celebra todos los años en febrero para concienciar y promover la importancia de la alfabetización y la educación en los medios de comunicación. En los Países Bajos, la asociación Mediawijzer.net ha examinado el resultado de todas las acciones, para una Internet más segura, propuestas en los últimos 10 años. También preguntó a 21 artistas, científicos, empresarios, desarrolladores, filósofos e incluso a un destacado hacker qué tipo de alfabetización mediática necesitamos en el futuro. El resultado es un libro (en inglés) lleno de ideas e inspiración. En Suecia *MIL for Me*<sup>22</sup> reúne una serie de módulos de aprendizaje en línea y planes de lecciones para maestros y bibliotecarios sobre conocimientos básicos de medios de comunicación e información. Insafe ha traducido al inglés un capítulo sobre la presentación de informes en línea. UK - *Childnet*<sup>23</sup>, socios del Reino Unido *Safer Internet Center*, revelado *Trust Me* el año pasado. Es un recurso diseñado para apoyar a los maestros de escuelas primarias y secundarias en la exploración del pensamiento crítico en línea. El Consejo de Europa ha publicado un manual de alfabetización en Internet a finales de 2017<sup>24</sup>. El manual ofrece una visión general de las consideraciones éticas y los riesgos asociados al intercambio de información y recursos. Los países europeos muestran un alto grado de conciencia sobre el robo de datos y los problemas de seguridad en línea.

### **1.3.3. Acoso en línea**

El acoso, cibernético o no, se define como el comportamiento que hace que alguien se sienta molesto, incómodo o inseguro. Este es usualmente un comportamiento deliberado y puede tomar formas verbales, indirectas y físicas. El acoso cibernético es el intento de ofender, amenazar, bloquear o acosar a otros utilizando dispositivos técnicos como Internet y los teléfonos móviles. El autor, también llamado matón, busca una víctima que no pueda defenderse de los ataques. Por lo tanto, existe un desequilibrio entre el perpetrador y la víctima, que es explotada por el perpetrador. La víctima suele estar socialmente aislada. El ciberacoso se produce en Internet, con mayor frecuencia en redes sociales, portales de vídeo,

---

<sup>22</sup> <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=716671>

<sup>23</sup> <https://www.childnet.com/resources/trust-me>

<sup>24</sup> <http://www.europarl.europa.eu/factsheets/it/sheet/138/politica-audiovisiva-e-dei-media>



etc., incluso a través de aplicaciones de mensajería instantánea como WhatsApp. A menudo el matón es anónimo, por lo que la víctima no sabe exactamente de quién vienen los ataques. Sin embargo, el acoso cibernético entre niños y adolescentes suele estar asociado con el entorno personal "fuera de línea", como la escuela, el vecindario residencial, el pueblo o la comunidad étnica. En algunos casos el acoso empieza en línea y continúa fuera de línea en la escuela, o viceversa. Por lo tanto, en la mayoría de los casos, el acoso y el ciberacoso no pueden considerarse problemas separados. El fenómeno de la intimidación siempre ha existido y se ha combatido, a menudo eficazmente, hasta el punto de reducir su incidencia y gravedad de manera significativa. El acoso cibernético puede considerarse el mismo fenómeno, pero utiliza otros canales de difusión, como la Internet, siendo, de hecho, mucho más difícil de erradicar (Tonioni, 2014). En primer lugar, los atacantes, los ciber-acosadores, son más difíciles de identificar (Buccoliero & Maggi, 2017) gracias a la posibilidad de crear perfiles falsos. En segundo lugar, el público objetivo es mucho mayor, con las consecuencias perjudiciales que se conocen o se pueden imaginar. El atacante puede involucrar escuelas, ciudades y pueblos enteros con un clic. Además, la víctima puede ser atacada a través de formas de ciberacoso las 24 horas del día, en cualquier momento del día sin tener aliento. Un fenómeno que atrae la atención de los medios de comunicación sólo cuando llegan a las noticias episodios con consecuencias dramáticas. El informe de ISTAT *Il Bullismo in Italia: comportamenti offensivi e violenti tra i giovanissimi* de 2015 revela eso: "En 2014, poco más del 50% de los niños de 11 a 17 años sufrieron (offline-online) algunos episodios ofensivos, irrespetuosos y/o violentos por parte de otros niños o niñas en los 12 meses anteriores. El 19,8% son acosados asiduamente porque son acosados varias veces al mes. El 9,1% de los actos de intimidación se repiten semanalmente" y, además, "el 63,3% de los niños y adolescentes han presenciado el acoso de unos niños contra otros en los 12 meses anteriores". El 26,7% afirma haber sido testigo una o más veces al mes» (Domenici, 2017).

#### **1.3.4. Sexting**

La red es también un lugar para socializar, para conocer a personas que comparten los mismos intereses, ideas o gustos sexuales. Es el lugar de lo "posible" para presentarse por lo que se es, o más fácilmente un lugar donde se puede crear una identidad alternativa. Una identidad mejor o peor, en la dirección de la idea, que poseemos, de la personalidad ganadora. Tratar de

alcanzar o encarnar un ideal diferente de la realidad es un nuevo desafío para los jóvenes. Los adolescentes de ambos sexos publican fotos en las que se ven perfectos, después de intervenciones más o menos invasivas con photoshop, snapchat, cara arriba y muchas otras. Los estándares aumentan y la brecha entre lo que realmente son y lo que parecen se vuelve insalvable. Permanecen prisioneros en la red, seres hermosos, infelizmente atrapados en sus propias mentiras. Incapaz de volver al mundo real donde el "yo" es demasiado banal y desgastado comparado con su alter ego virtual. La forma en que los adolescentes se comunican hoy en día no es tan diferente de la forma clásica. La reputación, en nuestro caso la de Internet, es muy importante. Pero a diferencia de ayer, es suficiente para avergonzar, lamentar, herir a alguien más. Un comentario fuera de lugar, dicho con superficialidad, es suficiente para desencadenar una serie de reacciones de avalancha y crear un caso cuyas consecuencias serán imprevistas. La red actúa como una caja de resonancia cuya vibración es imparable. Los canales de intercambio, legítimos y no, lo difundirán en el tiempo y el espacio. A esto se añade la desinhibición, a la que aporta una comunicación facilitada, que no permite ver la cara del otro ni leer y descifrar sus reacciones físicas o emocionales. Añadimos el hecho de que no se puede cuantificar o seleccionar con certeza el número de personas que leerán o verán lo que se ha publicado. Esto complica la comunicación y requiere una reflexión cuidadosa antes de publicar cualquier cosa en línea. Las crónicas de hoy nos recuerdan, sin embargo, que esta sabia y consciente cautela se consigue a menudo más tarde, cuando ya es demasiado tarde para remediarla, y la ingenuidad se ha pagado un alto precio. El sexting forma parte de estos comportamientos, a veces ingenuos e imprudentes, desgraciadamente comunes entre los adolescentes, que son seguidos por consecuencias muy desagradables para sus autores.

El término sexting es un neologismo y se refiere al envío de imágenes íntimas desnudas o semidesnudas. A menudo los adolescentes más o menos consentidos son forzados por sus compañeros o, peor aún, como adultos con perfiles falsos, a compartir imágenes en actitudes íntimas o con poca ropa. Una vez que el vídeo o la imagen se ha compartido, hay muchas formas de chantaje: solicitudes de dinero, fotos más atrevidas, amenazas de seguir compartiendo, y así sucesivamente, hasta que la víctima, de espaldas a la pared, encuentra el valor para pedir ayuda o comete un acto imprudente y dramático para poner fin al chantaje. Las fuerzas del orden reconocen que, en muchos casos, el sexting lo realizan bandas criminales que ganan millones de euros con estas acciones ilegales. A menudo, los chantajistas trabajan en equipos organizados y reciben una bonificación si logran extorsionar

más dinero de las víctimas designadas. Estas acciones constituyen el delito de sextorsión, extorsión y coacción sexual en línea y son un delito penal.

### **1.3.5. Riesgos de los dispositivos informáticos**

El primer virus informático se remonta a Fred Cohen, un investigador estadounidense que en 1983 pudo crear un software capaz de reproducirse automáticamente. Desafortunadamente, esta idea comenzó a extenderse, creando las llamadas infecciones en línea. En 1984 A.K. Dewdney (1985) creó un juego *Core War*<sup>25</sup> que implicaba el desafío entre programas con la victoria de uno capaz de destruir a todos los demás. Sin embargo, desde el entorno lúdico, las nuevas ideas se desbordan hacia otras áreas y se convierten en verdaderos cibercrímenes. El virus es tal porque realiza dos acciones específicas: la reproducción, es decir, el apego a otros programas y dar lugar a una acción, generalmente perjudicial (Messi, 1992). Lo que llamamos un virus informático entra dentro de la definición más general de malware o "software malicioso". El malware es creado por los programadores a veces con fines recreativos, pero mucho más frecuentemente por razones económicas. Porque, al infectar una computadora, te permiten hacerlo:

- Robar contraseñas de sitios y códigos de tarjetas de crédito;
- Crear redes (Botnets) para alquilar para ataques DDOS u otras ilegalidades;
- Enviar spam con contenido publicitario;
- Alterar los clics de los banners publicitarios;
- Enviar correos electrónicos de phishing para estafas y reciclaje;
- Realiza escuchas (ciber-tapado).

Reconocer una ciberamenaza antes que el ordenador es la acción correcta y más eficaz para derrotar a tiempo el malware. Este tema está relacionado con la sección sobre la protección de los dispositivos informáticos tomada del cuestionario para los estudiantes de esta

---

<sup>25</sup> <http://www.linuxfocus.org/Italiano/September2002/article255.shtml>

investigación. ¿Cómo se infectan nuestros ordenadores? Hay muchas maneras en las que nuestros ordenadores pueden ser infectados.

Los programas maliciosos<sup>26</sup> más comunes son:

- El Caballo de Troya es un archivo aparentemente saludable que esconde, en cambio, malwares (por lo general, estos archivos son crackeados o descargados de par en par);
- Páginas web que explotan algunas vulnerabilidades del navegador o algún plugin;
- Unidades flash USB infectadas;
- Phishing o correos electrónicos de ingeniería social, donde el usuario es persuadido para instalar malware bajo falsas pretensiones.

Una vez que se ha producido la infección, los ciberdelincuentes tienen el control del ordenador de las víctimas, llamado, a partir de ahora, *zombie* o *Bot* (Kwon, Lee, & Lee, 2011). Mientras el desprevenido operador no realice ninguna acción en su PC, el malware permanecerá en silencio. Cuando se active la red de robots, habrá una desaceleración, también casi imperceptible. En ese momento, la red de bots activa se alquilará a terceros con diversos fines (spam, phishing, anonimato en el delito, robo de información). Cuando la red de robots se activa, el malware instalado comienza a ejecutar las órdenes de sus creadores.<sup>27</sup>

### **1.3.6. Casos de noticias. La Blue Whale**

Un caso de terrible actualidad es el "juego" nacido en Rusia, Blue Whale Suicide Challenge, BWSC (Kumar et al., 2017) en el que participaron cientos de adolescentes que fueron inducidos a suicidarse saltando de un edificio, lo suficientemente alto como para no dejar ninguna posibilidad de supervivencia. También se indujo a las víctimas a dejar un testimonio en vídeo como prueba de su valentía, un documento que demostraba a un autodenominado curador que habían superado la última prueba. Los adolescentes siguieron un protocolo muy preciso que todos los protagonistas de este juego mortal debían seguir. La Ballena Azul es un ritual psicológico espantoso diseñado para difundirse en la Red y estructurado para inducir a las mentes de los adolescentes a una especie de depresión profunda que están convencidos de

---

<sup>26</sup> <https://www.ottimizzazione-pc.it/i-tipi-di-malware-piu-diffusi/#>

<sup>27</sup> <Http://nonaccademico.blogspot.it/2013/08/virus-informatici-cosa-sono-da-dove.html>

superar mediante el suicidio. Para gestionar esta compleja regulación existen administradores llamados curadores que a través de las redes sociales reclutan a las víctimas adolescentes (Kumar et al., 2017).

El nombre de Ballena Azul proviene del comportamiento de algunas ballenas que se suicidan encallando en las playas. Las reglas son 50, se llevan a cabo en 50 días y proporcionan, entre otras cosas, de:

- Cortar y enviar al curador fotos que documenten la aprobación de cada prueba;
- Despertarse por la mañana a las 4:20 a.m. y ver videos psicodélicos y de miedo, previamente enviados por el curador;
- Dibuja una ballena y sigue cortándote.

También si no eres capaz de seguir todas las reglas:

- Castigarse cortándose repetidamente,
- Escuchar música deprimente

El último día, establecido por el propio curador, la acción a tomar será de

- Saltar del edificio más alto de la ciudad.

Según los psicólogos rusos que se ocuparon del fenómeno, la metodología seguida por los organizadores recuerda la práctica del lavado de cerebro, destinada a manipular las mentes. Un reportaje de Hienas, un popular programa de televisión italiano de denuncia social, el 21 de mayo de 2017, lanzó una denuncia sobre la propagación del juego Ballena Azul desde Rusia, pero se extendió como un incendio forestal en Brasil, Gran Bretaña, Francia y ahora en Italia. El 4 de febrero de 2018, de hecho, en Livorno, un joven adolescente de 15 años se arrojó desde el edificio más alto de la ciudad, presumiblemente en un intento de superar el tercer y último nivel del juego, precisamente, el suicidio. El inventor del BWSC, Philipp Budeikin, fue encontrado y arrestado en mayo de 2017, en la casa de su madre en Rusia. Fue declarado culpable de instigar el suicidio de al menos dos adolescentes a las que Budeikin había descrito como "desechos biológicos". El Moscow Times escribe sobre ello. Según la prensa local rusa, no muestra ningún sentimiento de culpa o arrepentimiento por sus acciones y las vidas que ayudó a romper. El Mensajero confirma que Philipp Budeikin está detenido en la prisión de San Petersburgo. En la prisión se le unen las cartas de amor y apoyo enviadas por sus víctimas. Su sentencia, que le costó 3 años de prisión sólo por incitación al suicidio, no

representa el fin del terrible juego, ya que los casos de emulación se han multiplicado en todas partes del mundo. Sería apropiado dejar en el olvido los actos de este niño definido como problemático desde la infancia. Sin embargo, una mirada cuidadosa a la forma en que Budeikin ideó el loco desafío podría ayudar a los padres a comprender a tiempo cualquier comportamiento anormal de sus hijos, especialmente los preadolescentes. Con el aumento exponencial de los suicidios entre los muy jóvenes también en otros continentes, se han creado plataformas que tienen como objetivo contrarrestar y prevenir esta cada vez más extendida: *Olocausto 2.0*. Al año siguiente nació *Pink Whale*<sup>28</sup>, una plataforma diseñada para contrarrestar la Ballena Azul. Este también es un juego de desafíos pero de carácter opuesto y eso es para difundir lo bueno. Los participantes tendrán que someterse a pruebas que consisten en ayudar a los que son intimidados, en abrazar a los que tienen problemas, en escribir cartas de amor. La plataforma de la Ballena Rosa también invita a todos los padres a monitorear el comportamiento de sus hijos, especialmente los muy pequeños de 9 a 15 años, porque un clic equivocado en la Web puede hundirse en un mundo oscuro y peligroso.

#### **1.4. El primer paso: *on line safety***

Para la construcción de una Escuela Digital 3.0, la seguridad en línea es la piedra angular sobre la que construir la innovación. La Escuela, al abrirse a la red, no debe ceder ante un desbordamiento descontrolado de las prácticas informáticas con la consiguiente pérdida de papel y autoridad de la figura del docente. Las instituciones de formación deben preparar a los estudiantes para los nuevos retos que tendrán que afrontar, porque la competencia digital, y más aún la seguridad en línea, no es, como puede parecer, un proceso automático. El uso de las nuevas tecnologías no conduce automáticamente a la "sabiduría digital" (Prensky, 2012). Muchos procesos, relacionados con el contexto de la tecnología de la información, pueden ser compatibles, e incluso funcionales, con el aprendizaje de los contenidos curriculares. Internet, estamos de acuerdo con Jenkins (2010), puede ser un recurso productivo para la didáctica, al importar los nuevos conocimientos de multitarea, redes, simulación o juegos, dentro de los sistemas escolares, pero al mismo tiempo confiar "el proceso de educación sobre los medios de comunicación con el objetivo de perfeccionar y ejercer una conciencia crítica de los nodos

---

<sup>28</sup><https://www.secoloditalia.it/2017/05/la-risposta-al-blue-whale-21-regole-della-balena-felice-boom-tra-i-giovani/>

centrales de los nuevos conocimientos adquiridos" (Jenkins, 2010). La Educación de los Medios introduce el concepto de Seguridad en Línea. Sin embargo, este término no es fácil y claro de definir. Debe tener en cuenta, de hecho, varios factores inestables. El concepto, en general, se relaciona con el bienestar físico y psicológico de quienes navegan en entornos digitales, la seguridad de los datos personales, los dispositivos en uso y el medio ambiente. De hecho, en el análisis de la seguridad en línea debe tenerse en cuenta una amplia gama de variables como factores contextuales. Estos, de hecho, pueden afectar, de manera más o menos relevante, la seguridad y los riesgos que corren los jóvenes en los espacios en línea. En diversas investigaciones, véase Gasser, Maclay & Palfrey (2010), se ha identificado el "contexto de pertenencia" como un elemento pertinente para evaluar el nivel de competencia en materia de seguridad en línea que poseen los jóvenes. Contexto en el que identificaron varios factores responsables o implicados en la evaluación del curso del riesgo. Los investigadores se han movido en tres direcciones:

1. El contexto tecnológico, económico y de mercado;
2. El contexto cultural y educativo;
3. El contexto jurídico y político.

Estos, definidos como "parámetros de macronivel" (Gasser, Maclay y Palfrey, 2010), interactúan con otros factores denominados: "factores de micronivel" (como el entorno, los medios de acceso, las pautas de utilización y los niveles de competencia, la edad, el sexo, la condición social, el comportamiento de los compañeros y la mediación de instructores experimentados). De esto se desprende el límite del análisis en cuestión que permanece constantemente abierto y susceptible de mejoras y variaciones, tantas combinaciones como sea posible entre las variables indicadas. En lo que respecta al primer ámbito (tecnológico, económico y de mercado), no cabe duda de que las diferencias económicas, el grado de desarrollo tecnológico e industrial del país al que se pertenece, determinan o agravan algunos riesgos en comparación con otros. En un país pobre o en desarrollo, el acceso a Internet y la infraestructura para conectarse en línea son menores. Los riesgos serán menores, así como las oportunidades. La cantidad de recursos que la política decide asignar a la digitalización de la escuela no puede sino afectar a la seguridad en línea de los estudiantes. Por ejemplo, la mejora de la telefonía móvil sobre la línea fija, la elección económica y de mercado, conducirá, por supuesto, a políticas de seguridad en línea dirigidas a las aplicaciones de la telefonía móvil, y así sucesivamente. El segundo grupo de macrofactores, pertenece al

contexto legal y político. Las políticas liberales frente a las políticas de seguridad intervencionistas, por ejemplo, influyen en la producción de leyes laxas o intransigentes. La etapa de digitalización de las infraestructuras, las medidas de prevención y protección de los niños, la mayoría de edad, todos estos factores intervienen en la capacidad de un país para proteger a sus jóvenes en línea. Hemos reservado el tercer puesto para el grupo de macrofactores que nos toca más de cerca: el contexto educativo y cultural. Varios estudios comunicados por Gasser y otros (2010) confirman la interdependencia entre la educación y el uso de Internet por parte de los niños. Un estudio europeo vincula, de hecho, los altos niveles de educación con las mayores tasas de uso de la Internet. Una amplia gama de factores culturales determina el proceso de seguridad. Por ejemplo, el plazo en que se cree que ha terminado la infancia puede variar desde el punto de vista cultural e influir en las políticas de protección de la infancia. En nuestro trabajo atribuimos a este contexto, el contexto educativo y cultural, la responsabilidad de desarrollar en los estudiantes la competencia de la seguridad en línea. A fin de que la educación escolar se beneficie de los recursos en línea de una manera razonablemente segura, las instituciones educativas, ya sean formales o informales, deben abordar cuestiones que no pertenecen a su tradición y cultura, pero que pueden dar lugar a procesos y prácticas culturales muy eficaces y más atractivos (Jenkins, 2010). A pesar de los progresos realizados en la comprensión de los riesgos en línea y de las numerosas medidas prometidas en toda Europa, sigue abierto el debate sobre los beneficios de la introducción de la tecnología digital en la educación. Gran parte de las investigaciones sobre los conocimientos especializados en materia de seguridad en línea que poseen o no los jóvenes se han realizado principalmente en Europa occidental y América del Norte (Gasser y otros, 2010). Se ha prestado mucha menos atención al tema en los países con economías en desarrollo o emergentes. Este diferente grado de conocimiento debe tenerse en cuenta, ya que el acceso a la Internet es compatible en casi todos los países. Creemos que existe una navegación suficientemente segura y prudente, pero nunca será aleatoria o instintiva sino competente e informada. Creemos que la solución es una responsabilidad compartida entre las instituciones educativas y la familia. Los educadores de todos los tiempos. En una sociedad en la que la tecnología y el mundo en línea desempeñan un papel cada vez más importante en la vida de las personas, resulta evidente que las escuelas también deben mantenerse al día con las últimas tendencias sociales. Debe ofrecer las mismas oportunidades para enfrentar nuevos desafíos. La educación sobre seguridad en línea concierne a todos los ciudadanos y, por lo tanto, debería comenzar en casa, desde la edad preescolar. Los profesores también deberían



ser capaces de proporcionar a sus alumnos todas las herramientas que necesitan para enfrentarse al mundo online de forma responsable y civilizada.

## **CAPÍTULO II**

### **Intervenciones políticas y sociales para el desarrollo de habilidades digitales**

#### **2.1. Iniciativas en Europa**

Numerosos proyectos han sido promovidos por organismos gubernamentales, nacionales e internacionales, con el fin de facilitar el proceso de integración de las competencias digitales en los procesos de formación. El objetivo de estas intervenciones ha sido esbozar las directrices para asegurar la plena ciudadanía en la Sociedad de la Información para todos.

Ejemplos de ello son las acciones promovidas por los organismos gubernamentales de los Estados Unidos con el Plan Nacional de Tecnología Educativa, Washington 2005 (Paige, Hickok y Patrick, 2004) y por Gran Bretaña con la estrategia y prioridades de Ofcom para la promoción de la alfabetización mediática: una declaración, oficina de comunicación, Londres 2004 (Jenkins, 2010).

Igualmente admirables fueron las intervenciones propuestas por la Comisión Europea que emitió las Recomendaciones (Parlamento Europeo, 2006) el 18 de diciembre de 2006 sobre las competencias clave para el aprendizaje permanente. En el texto se invita a todos los países miembros a que elaboren estrategias coordinadas para lograr el objetivo común, a saber, la posesión de aptitudes, consideradas indispensables, por los ciudadanos europeos.

Las competencias clave se entienden como los recursos que todos necesitamos para la realización y el desarrollo personal, la ciudadanía activa, la inclusión social y el empleo. Las competencias identificadas por la Comisión Europea son:

1. Comunicación en la lengua materna;
2. Comunicación en idiomas extranjeros;
3. Competencia matemática y habilidades básicas en ciencia y tecnología;
4. Competencia digital;
5. Aprender a aprender;
6. Competencias sociales y cívicas;
7. Sentido de la iniciativa y el espíritu empresarial;
8. Conciencia y expresión cultural<sup>29</sup>.

La cuarta de las ocho competencias clave, que el Parlamento Europeo ha incluido, es la competencia digital, que está relacionada con el tema que estamos tratando. Esto se define como la capacidad de utilizar las tecnologías de la información con familiaridad y una actitud cautelosa y de evaluación. Las tecnologías impregnan la rueda de todos nosotros tanto en el lugar de trabajo como fuera de él, en las esferas personales y sociales. La Comisión Europea, de hecho, parece prever, o ya sabe, las dificultades que se encontrarán en este proceso de digitalización de las escuelas, y teme los riesgos a los que podrían exponerse los estudiantes, si no se les educa previamente y con prontitud en un uso crítico y selectivo de los nuevos medios. El 20 de agosto de 2009, de hecho, el Parlamento Europeo invitó a los Estados miembros a promover proyectos de educación sobre los medios de comunicación. Suecia, Irlanda y el Reino Unido se sumaron inmediatamente a la iniciativa integrando la educación sobre los medios de comunicación en los programas escolares (Gómez & Iania, 2013). Estas iniciativas son seguidas por otros países como Alemania, Francia, Hungría y Malta. Las directrices promovidas por la Comisión Europea apuntan a un proceso de actualización

---

<sup>29</sup> <https://www.anp.it/competenze-chiave-nuova-raccomandazione-del-consiglio-d'Europa/>

constante de los conocimientos y aptitudes de cada ciudadano, de manera que este pueda autogestionarse, es decir, adquirir modelos, motivación y capacidad de control autónomo, para el aprendizaje a lo largo de toda la vida (Jenkins, 2010). A estas iniciativas se añade la Agenda Digital para Europa, una de las siete iniciativas emblemáticas de Europa 2020 (Lázaro, 2013). La iniciativa se centra en el papel fundamental de las tecnologías de la información y las comunicaciones en la sociedad del conocimiento. Encontramos en el texto todas las referencias a las competencias digitales, indispensables para el crecimiento del mercado de trabajo (Tabla 1). Un extracto del documento muestra la alarma europea contra el creciente cibercrimen y otras prácticas delictivas. La Internet es una realidad fundamental de la cultura moderna y, al no poder prescindir de ella, es necesario proteger y controlar las redes para garantizar una navegación suficientemente segura (Cinque, 2012). Se han diseñado varios marcos de trabajo para poner en práctica los conocimientos electrónicos. Se han creado numerosos proyectos para todos los ciudadanos o grupos específicos (adultos, niños de 6 a 12 años, adultos pertenecientes a la tercera edad, profesores, estudiantes de diferentes órdenes y grados, etc.).

**Tabla 1**

*Resumen de propuestas europeas sobre competencia digital*

Nombre	Grupo de referencia	Resumen
ACTIC	Todos los ciudadanos a partir de 16 años	<p>ACTIC significa "acreditación de competencias en tecnologías de la información y la comunicación". Esta iniciativa está en curso en Cataluña y está dirigida a todos los ciudadanos mayores de 16 años.</p> <p>La alfabetización digital tiene que ver con el uso seguro y crítico de las tecnologías de la sociedad de la información, en el trabajo, el ocio y la comunicación.</p>
BECTA's	Todos los	Esta revisión proporciona un modelo para los maestros y

review of Digital Literacy	ciudadanos a partir de 16 años	estudiantes de escuelas primarias y secundarias. Se basa en el concepto de que la alfabetización digital consiste tanto en habilidades digitales como en habilidades de pensamiento crítico. También proporciona una revisión de la literatura y material de apoyo para profesores y estudiantes.
CML MediaLit Kit	Adultos	El Centro de Alfabetización Mediática (CML) proporciona el kit MediaLit y establece una estructura básica con cinco conceptos clave y cinco preguntas clave sobre la alfabetización mediática. El marco tiene como objetivo permitir a los estudiantes deconstruir, construir y participar con los medios de comunicación. Se considera un punto de referencia para profesores, bibliotecarios de medios de comunicación, desarrolladores de planes de estudio e investigadores.
DCA	Los estudiantes de la escuela secundaria	El marco de evaluación de la competencia digital (DCA) forma parte de un proyecto más amplio sobre "Internet y las escuelas: cuestiones de accesibilidad, políticas de igualdad y gestión de la información".  El marco propone una definición y conceptualización de la Evaluación de la Competencia Digital que está vinculada a una serie de pruebas, generalmente dirigidas a estudiantes de secundaria (15-16 años).
DigEuLit	Todos los ciudadanos	Este proyecto fue creado por la iniciativa de aprendizaje electrónico de la CE y dirigido por la Universidad de Glasgow con el fin de elaborar un marco para definir el concepto de competencia digital.
ECDL	Todos los ciudadanos	El ECDL es una autoridad líder en la certificación de habilidades electrónicas. Es una organización sin ánimo de

		<p>lucro que proporciona una certificación que va desde el nivel de principiantes hasta el nivel avanzado para profesionales. El objetivo principal del programa más popular (ECDL / ICDL) es el desarrollo de las habilidades y conocimientos informáticos necesarios para utilizar el procesamiento de textos, las bases de datos, las hojas de cálculo y las aplicaciones de presentación.</p>
eLSe-Academy	La tercera edad	<p>eLSe-Academy - e-learning for Senior Academy - se centra en el aumento de la participación social, la potenciación y la inclusión de los europeos de edad avanzada en la sociedad de la información, con especial atención a la reducción del aislamiento de las personas vulnerables. eLSe tiene por objeto desarrollar y poner a prueba un entorno de aprendizaje electrónico específicamente dedicado y adaptado a las necesidades de los estudiantes de edad avanzada.</p>
eSafety Kit	Niños de 6 a 12 años	<p>Más que una foto, esta herramienta es un kit preparado para que los niños y sus familias puedan concienciarse sobre los problemas de seguridad en Internet; y para apoyar el uso eficiente pero seguro de la tecnología. El objetivo del kit es desencadenar discusiones intergeneracionales entre padres e hijos.</p>
Eshet-Alkalai's conceptual framework	Todos los ciudadanos	<p>Este documento de Eshet-Alkalai informa sobre los diferentes aspectos de la alfabetización digital y las múltiples aptitudes que necesitan los ciudadanos para ser funcionales en la era digital. Propone un marco conceptual para aclarar las competencias pertinentes a la alfabetización digital.</p>
IC3 Internet and	Todos los ciudadanos	<p>El IC<sup>3</sup> certifica los conocimientos básicos críticos necesarios para el uso eficaz de las computadoras y la tecnología de</p>

Computer Core Certification		Internet necesaria para alcanzar los objetivos empresariales, ampliar la productividad, mejorar la rentabilidad y proporcionar una ventaja competitiva
iSkills	Adultos	La estructura de clasificación de iSkills afirma ser la única Prueba de alfabetización en tecnología de la información y las comunicaciones (TIC), que evalúa el pensamiento crítico y la capacidad de resolución de problemas en un entorno digital. El marco se basa en el reconocimiento de que tanto las aptitudes cognitivas como las técnicas son necesarias para las personas que desean asumir un papel funcional en una sociedad digital.
NCCA ICT Framework for schools in Ireland	Escuela primaria y secundaria	Este marco es una guía para ayudar a los profesores a integrar las TIC como un componente transversal para todas las materias. Apoya una visión de la alfabetización digital como la capacidad de crear, comunicarse y colaborar; organizar y producir información; comprender y aplicar el conocimiento de las funciones de las TIC; utilizar las TIC para pensar y aprender; y desarrollar una actitud crítica sobre el papel de las TIC en la sociedad.
Pedagogic ICT licence	Profesores	La Licencia Pedagógica de TIC ofrece a los profesores la oportunidad de actualizar sus habilidades en TIC e integrar las TIC y los medios como parte natural del proceso de enseñanza-aprendizaje de la escuela.  Este certificado se obtiene al completar con éxito las asignaciones en cuatro módulos principales y cuatro módulos opcionales.  El objetivo es utilizar las TIC y los medios para la enseñanza

		y el aprendizaje.
Information literacy project – Scotland	Escuelas secundarias	Este marco se desarrolló en Escocia con el fin de promover la comprensión y el desarrollo de la alfabetización informática en todos los sectores de la educación. Se llevó a cabo un programa piloto en las escuelas secundarias, donde la competencia informática se definió en términos de habilidades, conocimientos y comprensión
UNESCO ICT Competency Framework for Teachers	Profesores	Este marco tiene como objetivo definir diversas competencias TIC para los profesores, con el fin de permitirles integrar tecnologías en su enseñanza. El proyecto hace referencia a un conjunto de normas y directrices de competencia para la implementación de las TIC.

**Fuente:** Elaborado propia a partir de la revisión realizada por Ferrari (2012, pp. 25-28)).

En 2017 Microsoft publicó algunas investigaciones centradas en la civilización, la seguridad y la interacción en línea. La investigación se llevó a cabo tanto en adultos de 18 a 74 años como en jóvenes de 13 a 17 años. Había 14 países involucrados: Alemania, Australia, Bélgica, Brasil, Chile, China, EE.UU., Francia, India, México, Rusia, Sudáfrica, Turquía y el Reino Unido.

Esta investigación muestra que el 65% de los encuestados han sido víctimas de al menos una estafa o han estado expuestos a un riesgo en línea; en particular, el 43% de los encuestados se refieren a un contacto no deseado, y el 17% a un verdadero acoso en línea. Además, el 58% de los jóvenes de 13 a 17 años conocieron al perpetrador cara a cara en línea.

Los encuestados creen que Internet es, en general, un lugar seguro en el que se respetan las normas de convivencia ciudadana, pero revelan una gran preocupación por la seguridad futura. Con motivo del Día de la Internet más segura de 2018, Microsoft inició una búsqueda



más actualizada con los 14 países mencionados anteriormente, a los que se han añadido 9 más (Argentina, Colombia, Hungría, Irlanda, Italia, Japón, Malasia, Perú y Viet Nam). Para obtener estos resultados debemos esperar hasta el 9 de febrero de 2019 para el Día de Internet Seguro (SID) 2019. De conformidad con las indicaciones europeas, Italia también ha previsto la equiparación con otras naciones en el ámbito de la digitalización informática y, a tal fin, el Ministerio de Educación, Universidad e Investigación ha publicado el Plan Nacional de Escuelas Digitales (PNSD). El documento es la columna vertebral de La Buona Scuola (Vese, 2016). Este plan prevé la innovación del sistema escolar y la necesidad de la educación digital. En el Acta del documento podemos ver los datos de referencia europeos, en lo que respecta a las competencias digitales.

Italia se encuentra en la siguiente situación:

- 25° en Europa por el número de usuarios de Internet (59% de toda la población);
- 23° para las competencias electrónicas básicas (47%);
- 17° en conocimientos especializados sobre el ITC;
- 22° en el número de graduados en disciplinas científicas y tecnológicas (STEM).

También establece en el documento sobre la Buena Escuela que el gobierno italiano tiene la intención de invertir en: investigación, formación, didáctica, metodología y desarrollo de habilidades. Este proceso será, según el documento, un camino conjunto con el Garante de la Privacidad, que tendrá la tarea de asegurar que los datos personales se gestionen digitalmente. Los objetivos se referirán a una base común de habilidades digitales que los estudiantes tendrán que desarrollar. Las acciones propuestas en el documento de la Buena Escuela indican cierta preocupación por que los estudiantes puedan quedar solos y desarmados en una sociedad gestionada, no siempre de forma honesta, por los medios de comunicación social. De ahí la invitación a los profesores a que acompañen a sus estudiantes en el desarrollo de habilidades analíticas y críticas que les permitan desentrañar los a menudo oscuros meandros de la red. Los estudiantes italianos, recomienda la OCDE (Organización para la Cooperación y el Desarrollo Económico), deben adquirir habilidades críticas, autonomía de juicio, es decir, activar nuevos procesos cognitivos (De Feo & Pitzalis, 2014). En la primavera de 2016, tuvo lugar la primera fase de la actualización del marco común de referencia de las competencias digitales contenidas en el marco europeo DIGICOMP (Ferrari, 2013). DigComp 1.0 fue desarrollado por el CCI-IPTS (el Instituto de Prospectiva Tecnológica o IPTS, situado en

Sevilla, España, y es uno de los siete institutos del Centro Común de Investigación), para contribuir al desarrollo y la mejora de las aptitudes electrónicas de los ciudadanos. El documento indica una lista de 21 competencias divididas en habilidades de conocimiento y actitudes, encerradas en 5 áreas:

- Información;
- Comunicación;
- Creación de contenidos;
- Seguridad;
- Solución de problemas.

Prevé específicamente que los estudiantes, durante su educación escolar obligatoria, traten los siguientes temas:

- Los derechos de red, tal como se definen en la Declaración de Derechos de Internet, elaborada por el Comité de Derechos y Obligaciones de Internet de la Cámara de Diputados;
- Educación sobre medios de comunicación y dinámica social en línea (redes sociales);
- Calidad, integridad y circulación de la información (fiabilidad de las fuentes, derechos y deberes en la circulación de las obras creativas, privacidad y protección de datos, conocimientos básicos de información).

**Figura 1**

*Marco de alfabetización web editada por la Fundación Mozilla*



En Italia ya se han emprendido algunos caminos didácticos en este sentido por "Generazioni connessi", un proyecto desarrollado por el MIUR "en colaboración con el Ministerio del Interior-Policía Postal y Comunicaciones, la Autoridad Garante de la Infancia y la Adolescencia, Save the Children Italia, Telefono Azzurro, Universidad de Florencia, Universidad de Roma "La Sapienza", Skuola. net, Cooperativa E.D.I. y Movimento Difesa del Cittadino, Agenzia Dire, con el objetivo de dar continuidad a la experiencia desarrollada a lo largo de los años, mejorando y fortaleciendo el papel del Centro Italiano para una Internet más Segura, como punto de referencia a nivel nacional en lo que respecta a las cuestiones relacionadas con la seguridad en la Internet y la relación entre los jóvenes y los nuevos medios de comunicación"<sup>30</sup>.

<sup>30</sup> <https://www.generazioniconnesse.it/site/it/il-progetto/>.

Otro proyecto de interés es “Una escuela de OpenCoesione” (ASOC)<sup>31</sup> que es una propuesta educativa centrada en los siguientes ámbitos:

- Habilidades digitales;
- Educación cívica;
- La narración de cuentos.

El proyecto se inicia a través del desarrollo de habilidades transversales como: "el desarrollo del sentido crítico, la resolución de problemas, el trabajo en equipo y las habilidades interpersonales y de comunicación". Por primera vez en el año académico 2017/2018, los maestros que han probado su mano en este nuevo camino recibieron créditos de formación (Peterlongo, Recla, Ventura, Centonze, & Torri, 2010). Una rápida navegación por Internet revela la presencia de numerosos proyectos de capacitación, grupos de apoyo temáticos y guías prácticas sobre conocimientos digitales. Habilidades y destrezas para adquirir, entrenar, implementar. Sólo para nombrar algunos de los mejores que encontramos "Futuro Inteligente" de Samsung School<sup>32</sup>, que quiere experimentar un entorno altamente digitalizado con tabletas y pizarras electrónicas en 300 aulas. A esto se suman grupos temáticos en Facebook como “Insegnanti 2.0”<sup>33</sup>, “Il tablet a scuola”<sup>34</sup>, “La scuola nella nuvola”<sup>35</sup> y muchos otros. Los recursos para desarrollar aptitudes electrónicas invaden la red y se dirigen a todas las categorías y grupos de edad. Informamos, en resumen, de los objetivos de los principales proyectos digitales y educativos.

---

<sup>31</sup> <http://www.ascuoladiopencoesione.it/>.

<sup>32</sup> <https://www.samsung.com/it/aboutsamsung/sustainability/corporate-citizenship/education/smart-school/>.

<sup>33</sup> <https://www.facebook.com/insegnantiduepuntozero/>.

<sup>34</sup> <http://www.iltabletascuola.it/>.

<sup>35</sup> [http://www.mondodigitale.org/it/chi-siamo\\_temp](http://www.mondodigitale.org/it/chi-siamo_temp).

**Tabla 2.**

*Resumen de los proyectos digitales para una nueva didáctica ofrecida en la red*

Coding e Dintorni	Curso preparatorio que tiene por objeto servir de incentivo a la innovación de las aptitudes digitales en las escuelas, mediante la difusión y promoción de enfoques pedagógicos innovadores.
Anima digitale	Programa de formación gratuita para 8.000 animadores digitales de la escuela italiana.
Concorsi Digitali	Concursos organizados por la AICA junto con la USR y las Regiones, dirigidos a los estudiantes, para poner de relieve las habilidades digitales aprendidas durante el curso de estudio.
Rete DIDASweb	Plataforma digital creada y gestionada por DIDASCA que permite compartir el conocimiento, las habilidades, la creatividad y las buenas prácticas de todos los profesores de italiano, y no sólo.
Formazione e aggiornamento sulla Governance IT	Seminarios sobre la gobernanza de la tecnología de la información, la seguridad de la tecnología de la información y la gestión de los riesgos.
Progetto per i progetti	Seminarios de sensibilización sobre posibles amenazas mediante el aumento de la confianza en el uso de la tecnología. Centrarse en las oportunidades profesionales relacionadas con el uso de las herramientas de comunicación digital.
First Italian Week for Digital Cultural Heritage,	Seminarios y eventos en el territorio nacional para

Arts & Humanities EUCIP Core/e-CFplus Fundamentals nei Piani di Studio degli Istituti Tecnici Economici - SIA	concienciar sobre el valor de las culturas digitales.
WebTrotter - Il giro del mondo in 80 minuti	Concurso de equipos, dirigido a estudiantes de 15 a 17 años, cuyo objetivo es estimular la investigación inteligente en la web y el uso educativo de las herramientas digitales.
Ludoteca del registro. it	Ruta educativa de juego y aprendizaje que tiene como objetivo explicar a los niños y adolescentes cómo funciona la red, crear conciencia en su uso y destacar su potencial.
Abc digital	Proyecto que difunde la cultura digital y difunde el uso de herramientas relacionadas entre los nativos no digitales, involucrando a los estudiantes de secundaria y mejorando sus conocimientos de computación.
Progetto EduPuntoZero	Cursos cuyo objetivo principal es llevar el conocimiento del software científico y de aplicaciones directamente a los laboratorios de las escuelas para mejorar el currículum de los estudiantes en habilidades digitales.
Comprendere e valorizzare le Infrastrutture Digitali	Curso de alfabetización digital abierto a todos en el autoaprendizaje. Está disponible gratuitamente en la dirección:  <a href="https://learning.progressintraining.it/enrol/index.php?id=14">https://learning.progressintraining.it/enrol/index.php?id=14</a>

Social Media e Cyberbullismo	Un ciclo de conferencias sobre el ciberacoso para profesores, directores, estudiantes y padres, interdisciplinario gracias a la presencia de abogados, educadores, informáticos, psicólogos, periodistas.
Digital Capabilities and Social Capital	Proyecto piloto, que incluye una prueba de orientación sobre las habilidades digitales de los estudiantes de secundaria y una encuesta sobre el capital social de las familias.
"Alter Ego del Web" tra i banchi di scuola	Curso que da indicaciones y sugerencias para un uso correcto de la red con el fin de evitar sus escollos. El curso tiene por objeto comprender cómo utilizan los jóvenes Internet, estimulando la comparación con los padres, con la participación de la Escuela y las Instituciones.
EducationLab	Seminarios en un entorno de aprendizaje colaborativo CLE. La plataforma ofrece un contexto de aprendizaje en el que se facilita la interacción comunicativa entre diferentes sujetos: alumnos, profesores, expertos, facilitadores.
Ragazzi nella Rete	Reuniones para ayudar a los padres y a los niños a usar Internet conscientemente, evitando sus peligros y trampas.
Consapevolezza digitale	Proyecto que tiene por objeto sensibilizar a los estudiantes de enseñanza secundaria sobre el uso adecuado de los medios digitales, en particular las computadoras, los teléfonos inteligentes, las tabletas, las consolas de juegos, los lectores electrónicos, etc.

Para los profesores, hay una variedad interminable de recursos educativos y de concienciación digital disponibles en línea. Por ejemplo, en la sección de recursos del portal *Better Internet for Kids (BIK)*<sup>36</sup>, puedes encontrar tanto recursos de texto como de vídeo sobre muchos temas, divididos por las lenguas de la UE.

Otros ejemplos son:

- *Crossing the Line* - un práctico kit de seguridad online, de la *United Kingdom Safer Internet Center*<sup>37</sup> con películas y lecciones simuladas para alumnos de 11 a 14 años. El objetivo de este conjunto de herramientas es ayudar a los educadores a generar debates entre los jóvenes sobre sus experiencias en línea. Aborda temas como el ciberacoso, el sexting, la presión de los compañeros y la autoestima;
- Manual de Internet y sexualización temprana. Esta guía y el plan de lecciones de *Bulgarian Safer Internet Center*<sup>38</sup> proporcionar información sobre una serie de cuestiones en línea. Con consejos sobre cómo discutir los problemas en clase. La guía se apoya en varias lecciones de muestra;
- *La guía para el ciberacoso es un folleto de la Safer Greek internet center*<sup>39</sup> que proporciona consejos y asesoramiento sobre cómo evitar el ciberacoso y qué hacer en caso de que te encuentres con él;
- *La protección de la privacidad en las redes sociales es un folleto para los jóvenes de Slovenian Safer Internet Center*<sup>40</sup> que se ocupa de cuestiones de cómo proteger la privacidad en las redes sociales;
- *No es gracioso, duele. Este es un recurso de video de Safer Internet Cente UK*<sup>41</sup> que ayuda a los jóvenes a comprender los desafíos de la vida en línea y el impacto que los comentarios negativos pueden tener en otros.

Sin embargo, junto con el uso de recursos personalizados, es importante que las conversaciones sobre seguridad en línea sean una parte integral de la programación educativa.

---

<sup>36</sup> <https://www.betterinternetforkids.eu/>.

<sup>37</sup> <https://www.saferinternet.org.uk/>.

<sup>38</sup> <https://www.safenet.bg/en/>.

<sup>39</sup> <https://www.betterinternetforkids.eu/web/greece/profile>.

<sup>40</sup> <https://www.betterinternetforkids.eu/web/slovenia/sid>.

<sup>41</sup> <https://www.saferinternet.org.uk/>.



Estos proyectos, y muchos otros que se pueden encontrar en la red, han sido utilizados por un número limitado de instituciones educativas el MIUR, de hecho, en 2015, a través del Plan Nacional de Escuelas Digitales, se habla de "convocatoria abierta" a investigadores y expertos para implementar lo digital en las escuelas.

En septiembre de 2017, los resultados esperados y los compromisos asumidos parecen estar todavía en curso, como lo confirma el Ministerio de Educación (MIUR). Luca Annunziata (Editor de Startup Italia) ha presentado una nueva propuesta, a saber, la creación de tres mesas de trabajo:

- El método BYOD a lo largo del ciclo escolar. (BYOD significa "Bring Your Own Device" y generalmente se refiere a las políticas de la empresa que permiten a los empleados llevar y usar su smartphone, tablet o portátil en el lugar de trabajo. En la escuela se refiere a las nuevas y esperadas políticas que permiten a los estudiantes utilizar sus dispositivos de computadora personal en el aula);
- La cartografía de las metodologías de enseñanza innovadoras (es un proyecto que tiene por objeto crear un marco, lo más completo y exhaustivo posible, sobre las metodologías de enseñanza digital. El proyecto es implementado de manera espontánea y autónoma por los propios profesores que comparten su experiencia de enseñanza con lo digital. Los recursos están disponibles para todos;
- La revisión de los programas nacionales.

Y promete iniciar otras mesas para desarrollar proyectos:

- Ciudadanía Digital;
- Pensamiento computacional;
- Promoción de STEM (temas científicos);
- Educación empresarial<sup>42</sup>.

---

<sup>42</sup> Texto completo en:  
(<http://ischool.startupitalia.eu/education/60619-20170801-pnsd-la-tabella-marcia-della-scuola-digitale>)

## 2.2. Iniciativas en Italia

Las indicaciones europeas también se han transpuesto en Italia con nuevas disposiciones ministeriales. La Agenda Digital Italiana representa el conjunto de acciones y normas para el desarrollo de las tecnologías, la innovación y la economía digital. digital<sup>43</sup>. Esta propuesta es una de las siete iniciativas emblemáticas de la estrategia Europa 2020. En ella se establecen objetivos de crecimiento en la Unión Europea que deben alcanzarse para el año 2020 (Decaro, 2011). Bajo la égida de Europa, Italia ha desarrollado su propia estrategia nacional, identificando prioridades y métodos de intervención, así como indicadores específicos para medir el logro de los objetivos fijados, en consonancia con los cuadros de indicadores de la Agenda Digital para Europa. Con la contribución de la Conferencia de Regiones y Provincias Autónomas, la estrategia italiana se ha elaborado centrándose en la colaboración entre los niveles nacional y regional, y entre las propias iniciativas regionales. La Agencia para la Italia Digital (AgID, el organismo técnico del Presidente del Consejo que tiene la función de garantizar el logro efectivo de los objetivos de la Agenda Digital Italiana y colaborar en la difusión de buenas prácticas digitales, para la innovación y el crecimiento económico) también tiene la tarea de asegurar el logro de los objetivos italianos en coherencia con los europeos. En el marco del Acuerdo de Asociación 2014-2020, la Presidencia del Consejo, junto con el Ministerio de Desarrollo Económico, la Agencia Digital Italiana y el Organismo de Cohesión, ha preparado los planes nacionales:

- "Plan Nacional de Ultra Banda Ancha".
- "Crecimiento digital" (Matteucci, 2015).

La Agenda se estableció el 1 de marzo de 2012 tras la firma por todos los Estados Miembros de la Agenda Digital Europea, presentada por la Comisión Europea en 2010. En aplicación de la Directiva del Presidente del Consejo de Ministros<sup>44</sup>, del 1 de agosto de 2015, se publicó un documento que contiene las directrices de seguridad de las TIC para las administraciones públicas. El objetivo es proporcionar a las Administraciones criterios de referencia para establecer si el nivel de protección ofrecido por una infraestructura satisface las necesidades operacionales y también la intención de identificar las intervenciones más adecuadas para su

---

<sup>43</sup> <http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana>.

<sup>44</sup> <http://www.agid.gov.it/notizie/2017/04/07/pubblicata-gazzetta-ufficiale-misure-minime-sicurezza-informatica-pa>

posible adaptación. Este documento, dado el preocupante aumento del número de eventos de agresión cibernética contra la Administración Pública, invita a todas las Administraciones a adherirse a unos estándares mínimos de prevención contra los eventos cibernéticos. La adaptación de las Administraciones Públicas debe tener lugar antes del 31 de diciembre de 2017, a más tardar el gerente de la estructura responsable de la organización, innovación y tecnologías a que se refiere el artículo 17 del C.A.D. (Código de Administración Digital), o en su ausencia, por el Gerente designado a tal efecto. A fin de facilitar este proceso, el Organismo para Italia se ha comprometido a poner a disposición los indicadores de las normas de referencia, en consonancia con los que poseen los principales asociados de Italia y las organizaciones internacionales en las que Italia es parte. La Agenda promueve, como primer objetivo, la difusión de conocimientos digitales para las empresas, los ciudadanos y la Administración Pública. La Estrategia de Crecimiento Digital dedica, de hecho, un capítulo entero a las habilidades digitales. El programa consiste en un proyecto para acelerar la transformación digital del país, centrándose en una fuerte sinergia entre los sectores público y privado. La Coalición para las Competencias Digitales, en consonancia con el proyecto europeo Gran Coalición para los Empleos Digitales (Tullini, 2015) actualmente concluido, y del que AgID ha sido la referencia italiana, es el instrumento para promover y apoyar las iniciativas de alfabetización digital. Las actividades de la AgID tienen por objeto desarrollar las aptitudes digitales básicas, el liderazgo electrónico y las aptitudes especializadas, prestando especial atención a las nuevas profesiones y al mundo de las pequeñas empresas. Desde 2017, AgID también se encarga de apoyar la definición de las competencias digitales de los profesionales que trabajan en el sector de las TIC y de los que utilizan las TIC en sus actividades laborales. En junio de 2017 se publicó el informe del observatorio de aptitudes digitales 2017 realizado por Aica, Assinform, Assintel, Assinter (las 4 principales asociaciones de empresas de TIC que operan en el mercado italiano) en colaboración con la AgID y el Ministerio de Educación, Universidad e Investigación (Mereu & Franceschetti, 2018). Las nuevas tecnologías, como dijimos en los capítulos anteriores, representan una revolución, un punto de inflexión entre lo que fue antes y lo que será después. En particular, las redes representan un nuevo instrumento de creación de valor social. Digitalizar la administración pública, por lo tanto, significa proponer una nueva forma de hacer administración pública, porque las tecnologías son portadoras de nuevos estilos de vida, nuevas formas de ser competitivos. Italia, con las nuevas estrategias digitales a las que invita la Agenda Digital, participa en esta ola de innovación. Con este fin, Italia también ha previsto

una política de apoyo a la innovación, en todas las direcciones, desde la formación hasta la difusión de nuevas tecnologías, empezando por el aspecto reglamentario. La innovación trae consigo un valor social añadido en términos de calidad de vida, progreso cultural, nuevas oportunidades de trabajo, salud y educación. También es una herramienta a favor de la inclusión social y el despertar económico, ya que crea nuevas figuras profesionales (Bossi & Scellato, 2005) La inclusión de las competencias digitales, añaden los dos autores, es uno de los mayores retos de nuestro tiempo, y significa, de hecho, crear el requisito previo para la ciudadanía activa. Los conocimientos técnicos de los medios de comunicación, si están mediados por educadores expertos, permiten asumir, de hecho, una posición crítica ante la información disponible, adquirir un uso responsable de los medios de comunicación, así como promover nuevos intereses culturales, profesionales y sociales. La escuela es la primera avanzada de esta transformación, donde se compromete a promover el aprendizaje basado en el uso consciente de los lenguajes multimedia y a eliminar los obstáculos a un uso democrático de los recursos de la red en un sentido global.

Los conocimientos informáticos, desarrollados de manera no autónoma y desordenada, pero aplicados y forjados por expertos en enseñanza y capacitación, pueden salvar la brecha entre los modernos estilos de aprendizaje de los medios de comunicación y los procesos de aprendizaje de valores de la actividad escolar clásica. La teoría de la domesticación de Silverstone informa la metáfora en la que los animales salvajes se asimilan a los medios de comunicación, y revela la necesidad de domesticarlos, de familiarizarse con ellos para vivir con ellos: "la domesticación en el sentido tradicional, se refiere a la domesticación de los animales salvajes. A nivel metafórico podemos observar un proceso de domesticación, cuando los usuarios de diversos entornos se enfrentan a las nuevas tecnologías" (Silverstone, 2005).

### **2.3. Entrenamiento de seguridad en línea**

Por formación adecuada nos referimos a la información que parte de las amenazas online más habituales relacionadas con:

- La seguridad personal, como el ciberacecho, el ciberacoso y los depredadores en línea;
- La seguridad de la información, como el phishing, el robo de identidad y las estafas;
- Amenazas informáticas, como hackers, virus y otros programas maliciosos;

- Temas de contenido, como contenido obsceno u ofensivo.

No hace falta decir que la industria de la tecnología 2.0, al igual que los responsables de las políticas gubernamentales y los sectores de la comunicación, también tienen un papel clave que desempeñar y una responsabilidad civil y social que asumir. Uno de los últimos esfuerzos de política ha sido promover cursos de alfabetización mediática para los ciudadanos. En un intento de entrenar a los usuarios civilmente activos en una realidad que pasa a través de la lente a menudo deformante de los medios de comunicación. El desarrollo de la capacidad de pensamiento crítico es el recurso necesario para distinguir entre las fuentes de información fiables y la desinformación. En muchos países han surgido muchas iniciativas a nivel nacional para advertir a los jóvenes de los peligros de la utilización de las tecnologías en línea. Los periodistas de Le Monde en Francia y de la BBC en el Reino Unido fueron los primeros en Europa en desarrollar recursos que pueden utilizarse en las escuelas, subrayando el papel clave de las escuelas en la difusión de materiales de información sobre el tema. Las escuelas y los maestros, subrayan los publicistas, pueden desempeñar un papel crucial en la construcción de la resistencia de los jóvenes a las noticias falsas. Para hacer frente a la desinformación, se debería ofrecer a los navegantes en línea conocimientos y herramientas para hacer frente a la amplia gama de problemas que surgen en el uso cotidiano de los recursos de Internet; como el abuso en línea, el ciberacoso, el sexting, el establecimiento de falsas relaciones en línea como el bagre, el posible impacto negativo de la tecnología en la salud y el bienestar del usuario, los episodios de incitación al odio y la radicalización y, lamentablemente, mucho más. En Italia, el debate sobre la seguridad digital se abrió oficialmente en 2015 con las iniciativas del Ministerio de Educación, Universidad e Investigación (MIUR) para la innovación en las escuelas. El MIUR ha apoyado la necesidad de un cambio, a través de las tecnologías, en el sentido de desarrollo y adaptación a los estándares europeos. La iniciativa nació en oposición a quienes, en cambio, ven la autoridad de la información y la capacitación, sólo en las prácticas tradicionales del pasado.

A la luz de las modernas tendencias digitales, los órganos competentes y también la red, que actúa como ogro para un gran número de profesores y padres, han abordado una serie de cuestiones relativas a la navegación en línea. En primer lugar, el peligro que representan los extraños, que se pueden encontrar en las charlas públicas o en las redes sociales. El riesgo es concreto, pero estos peligros no son nuevos y no reemplazan a los reales, sino que son, si acaso, una extensión (Ito et al., 2010). En la diatriba entre admiradores y detractores del uso

de los recursos en línea, el debate, lamentablemente, lejos de haber encontrado una solución compartida, sigue abierto hoy en día en Italia y en Europa. En general, se trata de comprender mejor los riesgos y los desafíos que enfrentan los jóvenes al conectarse a Internet y de entender la importancia de proporcionar una navegación más segura y apropiada para los niños y los jóvenes. El imperativo es capacitar la capacidad de autorregulación y, por consiguiente, el acceso a los recursos en línea de manera cada vez más frecuente y segura, de modo que no tengan que renunciar a explorar las oportunidades que ofrecen los recursos en línea, a acceder a los vastos conocimientos de los que se valen, a comunicar y a desarrollar las aptitudes y la creatividad. Se han tomado muchas medidas en Europa y en todo el mundo con este fin, como veremos en los siguientes capítulos.

### **2.3.1. Desafíos en línea**

Aunque muchos debates y recursos se centran en la seguridad en línea de los estudiantes, es fácil olvidar que es igualmente importante para el bienestar de los padres y los maestros. Las estadísticas muestran que la seguridad en Internet es un tema que no debe ser subestimado, para nadie. Según una encuesta reciente en Irlanda<sup>45</sup>, uno de cada cinco profesores, por ejemplo, dice que ha sido víctima de abusos en línea por parte de sus alumnos o de sus padres. Los adultos también se benefician de la tecnología y pueden contar con una variedad de niveles de experiencia. Muchos profesores informan que se sienten mal equipados para tratar las preguntas y desafíos de los alumnos sobre temas de seguridad en línea. Más de dos tercios de los profesores encuestados en la misma encuesta (el análisis del Centro Nacional de Tecnología en la Educación (ncte) del proyecto de consultoría dot.safe farrell grant sparks - pdf.) dicen que no se sienten capaces de enseñar a sus alumnos sobre la seguridad en línea. Con ese fin, uno de los recursos más útiles es Insafe by Safer Internet Centers (SIC), un recurso que proporciona una enorme cantidad de información a los profesores para ayudarles a lograr un nivel de seguridad cada vez mayor en la gestión y utilización de los recursos en línea.

Toda la red es consciente del problema de la seguridad, de hecho se pueden encontrar, en todas partes, guías sobre cómo tratar problemas como el ciberacoso y el sexting, información lista para usar sobre seguridad y privacidad, decálogos de amplio espectro para principiantes y

---

<sup>45</sup> <https://www.irishexaminer.com/ireland/most-teachers-feel-unequipped-to-teach-online-safety-463234.html>

expertos. El portal Better Internet for Kids (BIK), por ejemplo, proporciona acceso a cientos de recursos en diferentes idiomas.

Sin embargo, aunque algunos recursos están en italiano, es necesario tener un nivel medio/alto de conocimiento del idioma inglés para poder navegar por el sitio, buscar recursos específicos y descargarlos. No hace falta decir que los adultos también deben prestar atención a su comportamiento en línea y en particular a su reputación en la red. Los profesores tienen derecho a la privacidad, pero el alcance de esa privacidad a menudo puede determinarse por la cantidad de contenido que se comparte en los medios sociales. Por ejemplo, una fotografía tomada durante una fiesta o evento social puede no crear necesariamente la imagen correcta de la persona que participó. Una fotografía es una fracción de segundo en el tiempo, pero la instantánea experimentada, quizás superficialmente, puede dar a otros la impresión equivocada de los sujetos retratados y causarles problemas, malentendidos y dudas que van mucho más allá de ese momento. Muchos empleadores también comprueban regularmente los perfiles de los medios de comunicación social y la presencia o ausencia en la web de posibles empleados, y las escuelas están haciendo lo mismo. En 2017, una profesora de inglés de 39 años, Lydia Ferguson, se vio obligada a dejar su trabajo porque publicó una foto en Facebook que se consideró demasiado sexy. Tras la dimisión de la profesora y a pesar de una petición que había reunido 250.000 firmas a su favor, un portavoz de la escuela en la que trabajaba se limitó a declarar: "Confirmamos que Lydia Ferguson ya no forma parte del personal de apoyo y que la escuela no tiene nada más que añadir"<sup>46</sup>.

Las redes sociales desempeñan un papel crucial en la gestión de las relaciones sociales, formales e informales. Debido a su carácter invasivo en todos los ámbitos sociales, la seguridad en línea debería enseñarse en escuelas y universidades como una asignatura independiente, en comparación con otras asignaturas. Los profesores deberían ser el primer puesto de avanzada para los estudiantes que buscan una navegación segura. Sin embargo, no lo son. Esto es confirmado por un reciente informe de UNICEF, que encuentra que sólo el 19% de los estudiantes dicen que confían en los profesores para resolver los problemas que se encuentran en línea. Esta parece ser una cifra relevante, dado que en el 80% de los casos, los propios estudiantes se consideran en peligro debido a los abusos, incluidos los abusos sexuales, perpetrados en línea<sup>47</sup>. Aún más alarmantes son las cifras de las recientes

---

<sup>46</sup> [Http://www.ilgiornale.it/news/cronache/foto-troppo-sexy-su-facebook-prof-si-dimette-1406363.html](http://www.ilgiornale.it/news/cronache/foto-troppo-sexy-su-facebook-prof-si-dimette-1406363.html)

<sup>47</sup> <https://www.unicef.org/endviolence/endviolenceonline>

investigaciones realizadas en Dinamarca, Hungría y el Reino Unido. Descubrieron que un número importante de jóvenes de entre 13 y 17 años no denuncian el acoso sexual en línea. El hecho de no denunciar el acoso se produce por diversas razones, entre ellas el temor a ser etiquetado por su participación en un hecho lamentable, a ser considerado como espía y también a que se le niegue el acceso a la Internet<sup>48</sup>. En la web hay disponible una interminable variedad de recursos educativos y de concienciación para maestros y padres. Sin embargo, estos recursos están casi todos escritos en lengua inglesa.

### Figura 3.

*Lista de los recursos más utilizados internacionalmente*

Crossing the Line	Safer Internet Center <sup>49</sup> , en el Reino Unido, sugiere un práctico kit de seguridad en línea, con películas y lecciones simuladas para explorar problemas en línea con alumnos de 11 a 14 años. El objetivo de este conjunto de instrumentos es ayudar a los educadores a entablar un diálogo abierto con los jóvenes sobre sus experiencias en línea. Los temas que se tratan incluyen el ciberacoso, el sexting, la influencia de los compañeros y la autoestima.
Handbook on the internet and early sexualisation	Handbook es una guía que proporciona información sobre una serie de temas en línea y consejos para los adultos sobre cómo discutirlos con los jóvenes.
Guide for Cyberbullying	Cyberbullying es un folleto del Centro Griego para una Internet más Segura que ofrece consejos y sugerencias sobre cómo evitar el acoso cibernético y qué hacer cuando uno se involucra.

<sup>48</sup> El proyecto de SHAME fue creado en colaboración con Childnet, Save the Children (Dinamarca), Kek Vonal (Hungría) y UCLan (Reino Unido), y está cofinanciado por la UE. Su objetivo es aumentar las denuncias de acoso sexual infantil en línea y mejorar la cooperación multisectorial en la prevención y la respuesta al acoso sexual infantil. <http://www.childnet.com/our-projects/project-deshame>

<sup>49</sup> [Http://www.childnet.com/resources/pshetoolkit](http://www.childnet.com/resources/pshetoolkit)



Protecting privacy in social networks	Protegiendo la privacidad es un folleto para niños del Centro Esloveno para una Internet más segura sobre cómo proteger su privacidad en las redes sociales.
It isn't funny, it hurts	"No es divertido, duele" es un recurso de vídeo del Centro para una Internet más segura que ayuda a los jóvenes a comprender los desafíos de la vida en línea y el impacto que los comentarios negativos pueden tener en la vida real.

Junto con el uso de recursos personalizados, es importante que las conversaciones sobre seguridad en línea sean una característica de la práctica en clase. En estos sitios se pueden encontrar muchas noticias que pueden ser utilizadas para estimular la discusión y el debate con los alumnos. Los recursos y consejos técnicos van acompañados de muchas historias, contadas por educadores y expertos en Internet. Las historias de casos reales muestran el poder de Internet y ofrecen una buena oportunidad para el debate y la discusión, de modo que los alumnos puedan comprender mejor las posibles consecuencias de las acciones en línea.

En algunos países existe la obligación de enseñar la seguridad en línea como parte del programa de estudios, pero esto no ocurre en todas partes, y menos aún en Italia, donde la función y las aptitudes del animador digital todavía se están definiendo y aplicando. Lo ideal sería que la seguridad en línea fuera una asignatura incorporada al plan de estudios en todas las asignaturas, no sólo durante las horas de computación. Ahora que somos conscientes de algunos de los retos a los que se enfrentan los jóvenes cuando se conectan a Internet, es importante que los profesores creen prácticas educativas en las escuelas, momentos dedicados en los que los jóvenes puedan hablar de estos retos y puedan buscar y obtener ayuda y apoyo para abordarlos. Actualmente, la brecha entre los adultos y los adolescentes es muy amplia. Por lo tanto, a los jóvenes les da mucha vergüenza hablar de lo que les pasa en Internet porque temen una reacción exagerada por parte de los padres y los profesores. Los adultos, de hecho, están bastante sorprendidos por lo que los jóvenes hacen o dicen en línea, en formas y contenidos que simplemente no pertenecen a la generación mayor. Es necesario capacitar a los adultos para que comprendan mejor las dinámicas que se generan en línea. Una sugerencia, tomada de numerosos maestros guías, sugiere una "visita guiada", tal vez por los propios adolescentes, sobre las tendencias de los nuevos medios de comunicación, los códigos

de conducta y los lenguajes de comunicación. Los profesores y los padres sólo podrán responder a las peticiones de ayuda de los adolescentes si son capaces de entrar en la dinámica de la red. European Schoolnet, a este respecto, ha elaborado una etiqueta de seguridad electrónica que los profesores y otros profesionales pueden utilizar para evaluar la forma en que se enfrentan a los problemas de seguridad en línea en su escuela. La etiqueta eSafety es un servicio de acreditación y apoyo en toda Europa para que las escuelas revisen sus prácticas de seguridad electrónica en función de las normas acordadas internacionalmente. Al presentar pruebas del desarrollo y la práctica de la competencia en materia de seguridad en línea, las escuelas pueden ser acreditadas como una escuela certificada en seguridad electrónica<sup>50</sup>.

### **2.3.2. Decálogo para educadores<sup>51</sup>**

Hay muchos decálogos en línea para padres y maestros que quieren educar a los niños y adolescentes en un enfoque saludable y responsable de los medios de comunicación. Los consejos y sugerencias provienen de investigadores, pedagogos, policías postales y expertos en tecnología de la información.

Algunas de ellas se han resumido en estas sencillas reglas y se han difundido en línea:

1. Inicie a sus hijos en el uso seguro de Internet pasando el tiempo navegando por las páginas web y redes sociales de uso común;
2. Edúquese y eduque a sus hijos en el uso sabio y consciente de Internet, estableciendo reglas y tiempos de conexión;
3. No confíe demasiado en los sistemas de protección y filtrado porque se pueden evitar, y sus hijos pueden navegar desde teléfonos móviles o en lugares públicos con Wi-Fi. Más bien, cuente con la educación y el desarrollo de habilidades críticas y de conciencia;
4. Cree oportunidades para hablar con sus hijos sobre cómo utilizar los recursos de la red. Averigua qué sitios visitan y con quién se relacionan;

---

<sup>50</sup> <https://www.betterinternetforkids.eu/web/esafety-label>

<sup>51</sup> <https://www.fondazioneveronesi.it/magazine/articoli/pediatria/navigare-sicuri-10-consigli-i-genitori-10-i-ragazzi> y <https://www.commissariatodips.it/da-sapere/per-i-genitori/navigazione-sicura-e-consapevole-dei-minori-su-internet.html>

5. Destaque los buenos sitios, resaltando su utilidad y los materiales que ofrecen. Anímelos a que le digan si han tropezado con sitios inapropiados, elógielos por decirlo y evite reacciones exasperadas si no se han comportado con seguridad. Tales reacciones podrían bloquear la comunicación;
6. Enseñe a sus hijos a usar los servicios más comunes de forma responsable, como: Facebook, Messenger, Youtube, incluyendo sitios de descarga de música y video. Enséñales a utilizar los recursos de Internet respetando los derechos de autor, la privacidad y la sensibilidad de los demás;
7. Aconséjales que acepten las amistades de las redes sociales sólo de personas que conozcan físicamente, que nunca entren en salas de chat para adultos y que informen a sus padres si se les pide que usen la cámara web;
8. Prepare a sus hijos para que no compartan información personal como la dirección, el número de teléfono, el correo electrónico y las fotos en línea. Nada, en resumen, que pueda hacerlos rastreables. Por supuesto, no les permiten conocer a gente que sólo conocen en Internet;
9. Anímelos a participar en otras actividades, deportivas, culturales y recreativas que no impliquen el uso de aparatos de computación;
10. Fomente buenas relaciones familiares y entable un diálogo sincero con sus hijos en los sitios que frecuentan.

Sin embargo, basta con recurrir a las buenas prácticas que forman la conciencia civil del ciudadano europeo en el camino hacia la aldea global. Muchos son los dictados y consejos que toma la red para orientar a los usuarios hacia un comportamiento basado en la prudencia y en relaciones sanas y respetuosas.

Ser amigable, acogedor y paciente es el primer paso.

- Cooperar para formar una comunidad que acoja y apoye a personas de todos los orígenes e identidades. Esto incluye, entre otros, a miembros de cualquier raza, etnia, cultura, origen, nacionalidad, color, condición de inmigrante, clase social y económica, nivel de educación, género, orientación sexual, identidad y expresión de género, edad, tamaño, condición familiar, política, creencias, religión y capacidad mental y física.
- Ser consciente y curioso sobre la diversidad para que represente un recurso y no un límite. Debido a esta diversidad, nuestra comprensión de cómo funcionarán las cosas

será diferente, nuestras referencias culturales y lingüísticas serán diferentes y tendremos soluciones muy diferentes a los problemas que discutimos. Es posible que una referencia subyacente no sea clara para otra persona y, como resultado, puede desencadenar un ciclo de malentendidos y descontento mutuos.

- Expresar una reflexión crítica amistosa y constructiva. Las críticas deben ir siempre acompañadas de sugerencias concretas sobre la forma en que se pueden mejorar las cosas y se debe considerar toda la información disponible sobre el tema del debate antes de expresarlas. Este, sin embargo, es un reflejo tan antiguo como el mundo, de hecho tan antiguo como el hombre. Ya sabemos que los proyectos que pongamos en línea serán utilizados por otras personas y nuestro trabajo puede a su vez depender del de otros. Cualquier decisión que se tome en línea influirá en otros usuarios cuyas reacciones darán lugar a otros comportamientos. Como en un proceso en cadena.
- Expresar la opinión en línea, aunque nos parezca impecable, no sólo dará lugar a un consenso. El desacuerdo, sin embargo, no puede ser usado como excusa para el mal comportamiento o los malos modales. Experimentar la frustración, por supuesto, nunca es agradable, pero no se puede permitir que esa frustración se convierta en un ataque personal.
- Acosar o tener un comportamiento excluyente no es, por supuesto, aceptable.

Las ocasiones en las que la broma o la diversión pueden resultar en verdaderos actos de persecución son muchas y aquí la intimidación, cibernética o no, se describe en detalle en sus peores declinaciones:

- Amenazas violentas o lenguaje dirigido contra otra persona...
- Bromas y lenguaje discriminatorio
- Publicar material sexualmente explícito o violento
- Publicar (o amenazar con publicar) información personal identificable sobre otras personas ("doxing")
- Los insultos personales, especialmente los que usan términos racistas o sexistas
- Atención sexual no deseada
- Promover o fomentar cualquiera de los comportamientos descritos anteriormente
- Acoso repetido a los demás;

- En general, si alguien te pide que te detengas, ¡detente!

La legislación sobre la privacidad ha intervenido para regular la conducta de quienes aún perseveran en el comportamiento ilícito. Profundizaremos en el próximo capítulo.

## **2.4. Legislación nacional y europea**

La difusión de Internet no ha ido acompañada desde el principio de una adaptación de las normas al respecto. Al leer el Informe sobre la innovación y las tecnologías en Italia (Italia. Ministerio de Innovación y Tecnologías, Oficina de Estudios, 2003), surge un fuerte sentimiento de inseguridad en el uso masivo de las Tics (Tecnologías de la Información y la Comunicación), de hecho, precisamente por su "falta de fiabilidad". En los años siguientes se intentó establecer una estrategia de reglamentación para seguir el ritmo de las nuevas tecnologías en materia de seguridad. Se crearon nuevos reglamentos para regular las relaciones económicas, sociales y jurídicas emprendidas en Internet. Estas normas se refieren en particular a "tres áreas diferentes":

- El económico, encargado de asegurar la eficiencia de los mercados, principalmente promoviendo el nivel adecuado de competencia entre los agentes económicos y evitando la aparición de antiguos y nuevos monopolios;
- Monopolios sociales, diseñados para proteger y defender a los ciudadanos, su salud, seguridad y el medio ambiente en el que viven;
- El jurídico, que regula el funcionamiento de los sectores público y privado definiendo las modalidades de las relaciones entre los diversos sujetos que forman parte de ellos". (Italia. Ministero per l'innovazione e le tecnologie, Ufficio studi, 2003).

A partir de hoy, la normativa italiana se ocupa de:

- Accesibilidad de los sistemas de información en la prestación de servicios, sin discriminación por motivos de discapacidad;
- Firma electrónica y valor legal;

- Protección de datos personales y nuevo código de protección de datos personales, que regula la materia e incorpora la Directiva 2002/58 de la Comisión Europea.

La Ley contra el acoso cibernético se promulgó el 17 de mayo de 2017. Se refiere a otro tema candente: el ciberacoso. El 17 de mayo de 2017, la Cámara Baja aprobó una ley contra el ciberacoso. La ley fue propuesta por la senadora Elena Ferrara, quien, durante su anterior actividad como profesora, había vivido en el drama de uno de sus alumnos los efectos del ciberacoso. La joven se quitó la vida en 2013, después de la publicación de un vídeo en el que fue acosada sexualmente. En Italia, hasta entonces, no había ningún marco reglamentario al que referirse. El único punto de referencia era el Telefono Azzurro (la ONG más importante que se ocupa de los menores) que formaba parte de un proyecto europeo de sensibilización sobre el tema. La ley dio, por primera vez, una definición oficial de ciberacoso entendida como:

"toda forma de presión, agresión, acoso, chantaje, insulto, menosprecio, difamación, robo de identidad, alteración, adquisición ilícita, manipulación, tratamiento ilícito de datos personales en perjuicio de menores, así como la difusión de contenidos en línea cuya finalidad intencionada y predominante sea aislar a un menor o a un grupo de menores mediante la comisión de abusos graves, ataques perjudiciales o burlas".

La ley<sup>52</sup> está dirigida principalmente a los menores y exige, en primer lugar, a los administradores de los sitios o redes sociales que eliminen el contenido no deseado en un plazo de 48 horas después de la denuncia; de lo contrario, el Garante de la Privacidad lo eliminará. Si el responsable tiene entre 14 y 18 años, no habrá un juicio sino sólo un "procedimiento de advertencia" (una serie de medidas disuasorias). Otras medidas se refieren a la prevención. Se creará una mesa técnica para prevenir y combatir el ciberacoso, bajo la responsabilidad de la Presidencia del Consejo. Cada escuela tendrá que designar una persona de contacto para iniciar los cursos de formación de los profesores para que tengan la capacidad de reconocer este tipo de comportamiento (Thiene y Marescotti, 2017).

---

<sup>52</sup> [www.gazzettaufficiale.it/eli/id/2017/06/03/17G00085/sg](http://www.gazzettaufficiale.it/eli/id/2017/06/03/17G00085/sg)

## 2.5. Safer Internet Day

El 6 de febrero de 2018 se celebró en Bruselas por 15º año consecutivo el Día de la Internet Segura de 2018. Al evento asistieron 140 países de todo el mundo. La reunión forma parte del Programa para una Internet más segura de la Comisión Europea y se renueva cada año. El evento está organizado por la red Insafe, coordinada por European Schoolnet (una red de 34 Ministerios de Educación europeos) e INHOPE (la Asociación Internacional de Línea Directa de Internet). European Schoolnet es una organización sin ánimo de lucro, cuyo objetivo es llevar la innovación en la enseñanza y el aprendizaje a los principales interesados:

- El Ministerio de Educación.
- Escuelas y profesores.
- Investigadores.
- Socios industriales.

La misión de European Schoolnet es apoyar la capacitación de los interesados en Europa en la transformación de los procesos educativos en una perspectiva digital. El objetivo de los miembros de la organización es

- Identificar y probar prácticas innovadoras
- Apoyar la integración de estas prácticas de enseñanza y aprendizaje de acuerdo con las normas del siglo XXI para la educación de todos los estudiantes.

La red conjunta Insafe e INHOPE de centros de Internet más seguros colabora para:

- Proporcionar una navegación más segura por Internet;
- Promuever el uso responsable de la Internet y los dispositivos móviles. Con especial atención a los niños, los jóvenes y sus familias;
- Identificar y eliminar el contenido ilegal en línea.

La Comisión Europea apoya a la red mediante la financiación proporcionada por el Servicio de Conexión con Europa (CEF). La Comisión Europea promueve una Internet más segura y mejor a través de la estrategia "Better Internet for Kids" que ofrece:

- Apoyo financiero a los centros de Safer Internet de todos los Estados Miembros, más Islandia y Noruega;
- Coordinación y financiación a nivel de la UE a través de la plataforma [betterinternetforkids.eu](https://betterinternetforkids.eu);
- Contribuciones a la creación de un marco reglamentario.

La Comisión también actúa como promotora de iniciativas de autorregulación, como la Alianza para proteger mejor a los niños en línea. Las celebraciones del Día de la Internet Segura (CEI) se llevaron a cabo el martes 6 de febrero de 2019. El eslogan de la campaña es "Juntos por una Internet mejor". Este lema es una invitación a todos los interesados a unirse y a desempeñar su papel en la creación de una mejor Internet para todos, y especialmente para los usuarios más jóvenes.



## **SEGUNDA PARTE**

### **MÉTODO, RESULTADOS Y CONCLUSIONES**



## **CAPÍTULO III**

### **Claves del entorno digital**

#### **3.1. Los sistemas de información para la escuela. Ejemplo de un sistema de gestión escolar**

El sistema de información del que vamos a hablar es la empresa líder en el sector de la gestión escolar, en cuanto a tecnología, recursos, facilidad de uso, seguridad y número de usuarios (institutos escolares de todos los niveles) que lo utilizan. El sistema aprovecha los entornos de desarrollo más avanzados para la web. Sus aplicaciones web permiten actualizaciones en tiempo real y garantizan la seguridad de los datos sin necesidad de hacer copias de seguridad continuas o de memorias externas adicionales. En su configuración en Red Local, los datos de información, introducidos en el sistema, fluyen en una única base de datos situada en un Servidor conectado en la Red a todas las computadoras, en las diferentes estaciones de trabajo, en las que operan varios programas de aplicación. Esa configuración agiliza los procedimientos de introducción de datos. De hecho, con un solo tecleo, la información se

pone a disposición de todas las solicitudes en los diferentes procedimientos. El sistema también presta servicios a las familias, a través de la web y por sms con un sistema capaz de garantizar la máxima seguridad y privacidad. Un sistema de control de acceso jerárquico garantiza la confidencialidad de los procedimientos utilizados por los distintos operadores previamente autorizados para gestionar datos específicos, utilizando claves de acceso y contraseñas personales, en cumplimiento de las normas de privacidad. Además, el sistema, gracias a la flexibilidad de su diseño, permite trabajar de manera autónoma y confidencial en su propia base operativa y transferir posteriormente los resultados del procesamiento a la base de datos centralizada. El modelo de seguridad y confidencialidad de los datos adoptado se inspira en los sistemas que se utilizan en el mundo bancario y financiero (PCI DSS). Esto se confirma por los estrictos controles de calidad impuestos por la norma ISO 9001.

### **3.2. Procedimientos de seguridad**

En lo que respecta a la seguridad informática de los registros electrónicos, la Oficina de Prensa de la Software-house, que examinamos, concedió esta entrevista a Orizzontescuola.it: "Nuestra empresa ha desarrollado todas las aplicaciones web para grandes volúmenes de tráfico (gestión de alumnos, encuestas, registro electrónico, pagos de presupuestos y, por tanto, la correspondiente gestión de datos sensibles), realizando periódicamente estrictas pruebas anti-intrusión y controles de seguridad de acuerdo con la norma internacional "PCI SSC Data Security Standards" (Payment Card Industry Data Security Standard) y la calidad exigida por la normativa vigente.

A pesar de la falta de obligaciones reglamentarias específicas, la Software-House ha decidido tomar como referencia el modelo de seguridad utilizado por las entidades que operan en el sector bancario / financiero. El protocolo de Capa de Conexión Segura (SSL), utilizado por nosotros, permite el acceso seguro a nuestro portal web. (Protocolo análogo ampliamente utilizado por las instituciones de crédito y los más importantes portales de comercio electrónico). Gracias a este protocolo de seguridad todos los datos de las escuelas, viajan por la web de forma encriptada, garantizando el más alto nivel de seguridad y confidencialidad, para proteger las transmisiones telemáticas. La presencia de este protocolo puede detectarse fácilmente por la escritura "http" que precede a la dirección de Internet a la que se está

conectado. La seguridad de las aplicaciones web producidas por nuestra Software-house está también garantizada por la gestión de las infraestructuras que nuestra empresa ha decidido no delegar en terceros, sino confiar a un amplio equipo de ingenieros de sistemas y programadores altamente especializados, dentro de la empresa y listos para intervenir de 7.00 a 23.00 hs.

Su tarea consiste en desarrollar y supervisar el funcionamiento de nuestros sistemas web para garantizar a los usuarios el más alto nivel de eficiencia y seguridad. No sólo eso, las diferentes granjas de servidores, elegidas por nosotros, es decir, las ubicaciones físicas donde se encuentran los datos, han sido seleccionadas a nivel nacional y europeo, después de haber demostrado la máxima fiabilidad y experiencia en seguridad informática y, en todo caso, después de haber verificado las medidas físicas, lógicas y organizativas puestas a cargo de la infraestructura informática. Como resultado de este compromiso de recursos, tanto financieros como humanos, podemos ahora afirmar con orgullo que ofrecemos a las escuelas los servicios web más seguros, fiables y eficientes, además de la tradicional completitud y simplicidad de uso de nuestras aplicaciones. Todo esto, junto con la pasión y la seriedad que ponemos en nuestro trabajo, ha decretado, en 25 años de actividad, el éxito y la gran difusión de nuestro software en la escuela italiana. Creemos, por lo tanto, que podemos tranquilizar a todos aquellos que nos han pedido aclaraciones y garantías en el campo de la seguridad.”<sup>53</sup>

### **3.2.1. Entrevista con el Vicepresidente de *Argo Software***

Después de una entrevista y numerosos contactos telefónicos el martes 15 de noviembre a las 11:30 a.m., el vicepresidente de la Software-house que hemos elegido, nos proporcionó una entrevista sobre Seguridad Digital.

Este es su punto de vista sobre la seguridad digital y el papel de los maestros y padres en la formación de los adolescentes.

*Tiziana Occhipinti*: "Buenos días ingeniero, su sistema con más de 5000 escuelas clientes en Italia ha logrado un papel de liderazgo en el diseño e implementación de software de gestión para las escuelas. En otras palabras, más del 70% de las escuelas italianas de todos los niveles

---

<sup>53</sup><http://www.orizzontescuola.it/argo-software-chiarisce-sua-posizione-merito-alla-sicurezza-del-proprio-registro-elettronico-sc/>

tienen software con su marca. En su sitio puede leer que entre las diez razones para elegir su software, puede encontrar protección de datos, privacidad, derechos de autor. Todos los conceptos de interés para nuestra investigación. Me gustaría preguntarle ¿con qué herramientas el Sistema garantiza la protección de la información introducida por los operadores de la escuela?"

Vicepresidente "Todos nuestros datos residen en servidores externos, protegidos por políticas de acceso con IP que son reconocibles por nuestros sistemas ("dirección IP" significa dirección de protocolo de Internet. Indica un grupo único de números que identifica a la computadora, lo que permite intercambiar datos con otras computadoras. En la actualidad, la mayoría de las direcciones IP consisten en cuatro grupos de números, cada uno de ellos separado por un punto: 192.168.1.42 es un ejemplo de una dirección IP). Además, ponemos en marcha políticas de respaldo continuo que garantizan la seguridad y la permanencia de los datos".

T.O.: "Una amenaza cibernética debe ser reconocida primero para que pueda ser contrarrestada. ¿Qué camino podría tomar el ciber-malware para acceder al servidor(es) que usas?"

V.P.: "Nuestro sistema no requiere que se descarguen aplicaciones para su uso; todo reside en un servidor accesible desde un simple navegador.

El problema de los correos electrónicos, de las aplicaciones descargadas, forma parte de una ética de comportamiento que concierne al cliente, es decir, al operador administrativo, al padre o al propio estudiante".

T.O.: "Así que los datos, sensibles y no, introducidos por las escuelas residen en un servidor remoto. ¿Son suficientes el antivirus, el cortafuegos y todos los sistemas de protección que utiliza para combatir los riesgos cibernéticos?"

V.P.: "Por las razones arriba mencionadas, creemos que sí."

*T.O.: "Bueno, la actualización de los sistemas también es parte de estos protocolos de seguridad. ¿Con qué frecuencia se actualizan los sistemas de protección contra el malware?"*

*V.P.: "Todo el paquete de sistemas operativos, y no sólo los sistemas de protección contra el malware, se actualizan tan pronto como se publica un nuevo pec. En cualquier caso, constantemente".*

*T.O.: "¿Con qué criterio recomienda crear las contraseñas?"*

*V.P.: "En realidad no damos consejos directos, ya que es el mismo sistema que obliga al usuario a utilizar combinaciones de letras mayúsculas y minúsculas asociadas a números y símbolos, por lo que guiamos al operador a una elección segura".*

*T.O.: "¿Cómo reconocer una amenaza cibernética?"*

*V.P.: "Tenemos un grupo de 5 operadores de sistemas que trabajan sin parar incluso en horas no laborables que operan un monitoreo continuo. Los operadores del sistema están equipados con una tableta de la empresa para poder comprobar el estado de riesgo potencial causado por una ciberamenaza incluso fuera de la empresa".*

*T.O.: "Una vez que publicas un contenido en Internet, sabes que siempre hay un rastro de él, incluso después de borrarlo. ¿Cómo se gestiona este riesgo al que están expuestos los datos?"*

*V.P.: "Necesitamos hacer una clara distinción entre las aplicaciones web y las aplicaciones sociales. Es obvio que cuando publicas algo en las redes sociales pierdes el control de ello. Sin embargo, esto (refiriéndose a nuestro sistema) es una aplicación web. De hecho, el usuario tiene un control completo sobre los datos registrados y puede editar, borrar y modificarlos a voluntad en nuestra nube. En cualquier caso, si una escuela decide rescindir el contrato con nuestra casa de software, todos los datos que le pertenecen serán devueltos al cliente y eliminados del sistema. No habría riesgo de pérdida de datos".*

*T.O.: "Los dispositivos electrónicos (desechos electrónicos) liberan metales tóxicos que pueden fluir hacia los vertederos y las aguas subterráneas. ¿Cómo manejar este tipo de residuos?"*

*V.P.: "En cuanto a los residuos de hardware que producimos, actuamos de acuerdo con una empresa certificada en la eliminación de residuos electrónicos. De esta manera, de una forma respetuosa con el medio ambiente, nuestro hardware obsoleto, o el que ya no se utiliza, se elimina o recupera adecuadamente o se reutiliza".*

*T.O.: "¿Qué es el DidUP - Solicitud de Familia?"*

*V.P.: "Es una aplicación multifacética que permite a las familias seguir el progreso del estudiante día a día y tener toda la información sobre el desempeño de las actividades*

educativas. El estudiante también tiene acceso a una especie de diario actualizado de las actividades escolares al alcance de la mano".

T.O.: "En este "diario" de actividades, ¿qué datos se pueden consultar?"

V.P.: "Los datos que están a disposición de los usuarios son: ausencias, retrasos, permisos, notas disciplinarias, temas realizados y tareas asignadas, justificación de las ausencias, visualización de las notas diarias y periódicas, informes electrónicos, tableros de anuncios, solicitud de certificados, reserva de entrevistas con los profesores, consulta de libros de texto. Casi todo."

T.O.: "Todo esto está disponible en dos tipos: alumno y padre. Los dos tipos, estudiante y padre, son administrados por la escuela. ¿Puede controlar su uso? Es decir, ¿en qué porcentaje se activa la tipología de los alumnos (por las escuelas), o se activa casi exclusivamente la tipología de los padres?"

V.P.: "Claro. Sabemos que el 30% de los usuarios generados son de tipo estudiante, el 70% restante de tipo padre."

T.O.: "¿Así que los estudiantes podrían conectarse a su software a través de dispositivos como teléfonos móviles y tabletas?"

V.P.: "Todos estos dispositivos son siempre conectables al sistema. Basta con que tengan un navegador para utilizar las aplicaciones web; además, aplicaciones como didapp o didap-family también se pueden descargar y utilizar tanto desde tabletas como desde teléfonos móviles".

T.O.: "¿Quién es responsable de la seguridad de los datos sensibles? ¿El Sistema, el Ministerio de Educación o la propia escuela?"

V.P.: "La seguridad tiene dos niveles: uno es la competencia de la escuela que es responsable de la publicación y el tipo de datos publicados. El segundo nivel pertenece a nuestro software que es responsable de su preservación".

T.O.: "Como expertos en la materia que operan en un centro neurálgico entre la escuela, los alumnos y la digitalización de ordenadores, ¿qué cree usted que se debe enseñar a los alumnos, durante la escolaridad obligatoria, sobre la seguridad digital?"



*V.P.: "En este tema soy muy crítico. Creo que los problemas son de dos niveles: uno se refiere a los profesores que a menudo no pueden enseñar seguridad informática porque no tienen la preparación adecuada para las necesidades que surgen al navegar. He podido comprobar en mi experiencia que muchos profesores, especialmente los más mayores, no muestran voluntad y disposición para aprender lo digital, al contrario, también he notado que para algunos de ellos es un motivo de orgullo haber resistido a la invasión de lo digital. No sé cómo es posible seguir siendo un extraño para él, pero así es como es.*

*En lo que respecta a los alumnos, creo que deberíamos empezar por lo básico. El hecho de que sepan utilizar las aplicaciones de Internet o los medios sociales no garantiza que puedan manejarse o protegerse. Por ejemplo, la información sensible que comparten en un chat puede propagarse y crear grandes problemas al propietario porque a partir de ese momento la información ya no es controlable. Puedo decir que los jóvenes carecen de sensibilidad ante el problema y alguien debería enseñárselos".*

*T.O.: "¿Su reflexión también concierne a las familias? Si es así, ¿qué deberían enseñar los padres a sus hijos sobre la seguridad digital?"*

*V.P.: "Me ocurre muy a menudo presenciar, por ejemplo en un restaurante, una situación como: niños alrededor de una mesa de restaurante, todos jugando con la tableta, colocados allí con la mirada alucinada de los padres pidiendo que los dejen en paz. Mientras los padres usen pastillas para este propósito, no podrán enseñar nada a sus hijos. No son capaces de enseñarles a defenderse de los peligros de la web, ni a usar sus recursos sabiamente, porque en primer lugar, Internet es una oportunidad, pero, tal como están las cosas, es sobre todo un peligro. Los padres deberían aprender primero a hacer malabarismos con el laberinto de Internet, tal vez capacitándose con cursos adecuados para ese fin, y luego dedicarse a sus hijos y a su capacitación en materia de seguridad digital.*

### **3.2.2. Entrevista con el Dr. Giovanni Gianni**

Viernes 29 de junio de 2018 entrevista con el Dr. Giovanni Gianni , especialista en medicina física y de rehabilitación, Director de Salud del Centro Especializado de Rehabilitación Físico-Médica de Ragusa, afiliado al sistema nacional de salud. El Dr. Gianni fue entrevistado para obtener información de primera mano sobre los daños causados a la salud por el uso

prolongado de Internet. El cuestionario que propusimos a los alumnos se refería a las lesiones por esfuerzos repetitivos y, de hecho, el Dr. Gianni nos respondió introduciendo las lesiones por esfuerzos repetitivos. Son patologías - dice el director - típicas de un uso prolongado del ordenador o de un uso excesivo. Estas lesiones afectan a los tendones y nervios de un determinado distrito articular. El movimiento continuo y siempre el mismo, prolongado en el tiempo, implica un esfuerzo muscular-articular no despreciable. El fenómeno afecta, en general, a las manos, las muñecas, los codos, los brazos, los hombros, pero también a la columna vertebral, con participación de la región lumbosacra. Estos pequeños traumas llamados lesiones por esfuerzos repetitivos, a diferencia de los traumas resultantes de un solo evento llamado agudo, se desarrollan lentamente con el tiempo, pero son igualmente incapacitantes. En cuanto a las actividades más fatigantes para los tendones y nervios de los miembros superiores y la columna vertebral, el Dr. Gianni cuenta entre las primeras víctimas a estudiantes, empleados y cualquiera que haga un uso prolongado de una postura incorrecta, en su escritorio, frente a una terminal de vídeo. Los mismos problemas que afectan, por ejemplo, a los trabajadores de la carretera, que utilizan martillos neumáticos (instrumentos con fuertes vibraciones), también conciernen a ciertos tipos de trabajo sedentario, que también se cuentan entre los de desgaste y causan lesiones por esfuerzos repetitivos. Trabajar en un terminal de vídeo, de hecho, representa un factor de riesgo porque mientras una parte de nuestro cuerpo permanece estática, o no muy móvil, los otros distritos, como el hombro, el codo, las manos se mueven incesantemente. Este contraste entre las posiciones estáticas y móviles puede dañar, al principio de forma microscópica, y luego macroscópicamente el aparato esquelético y muscular. Al descubrir la patología se requiere una intervención inmediata, ya que las microlesiones podrían, con el tiempo, resultar en una incapacidad permanente. En pocas palabras, la combinación de los siguientes factores puede provocar una lesión por esfuerzo repetitivo: la repetición de un gesto, como escribir en el teclado, los movimientos de la mano para utilizar el ratón, la fuerza con la que se escribe en el teclado, el mantenimiento de la misma posición, no intercalada con suficientes pausas, la asunción de una posición incómoda, un puesto de trabajo mal instalado en el que no se respete una distancia correcta entre la mesa y la silla, por ejemplo; o la colocación incorrecta del terminal de vídeo con respecto a la cabeza. Todo esto puede resultar anti-ergonómico, poniendo a los músculos peligrosamente bajo tensión. En cuanto a los síntomas más comunes de las patologías relacionadas con la mala postura. Gianni habla de: dolor genérico, rigidez muscular, crepitación articular (que son ruidos para fisiológicos que indican que algo a nivel

articular no funciona de manera fisiológica), dolor de acupresión, parestesias, hormigueo, pérdida de fuerza muscular, pérdida de rango articular, con la consiguiente falta de coordinación, por lo tanto, una pérdida de propiocepción, es decir, la capacidad de percibir y reconocer la posición del cuerpo en el espacio y el estado de contracción de los músculos, independientemente de la visión.

La falta de propiocepción asume una importancia fundamental en el complejo mecanismo de control de los movimientos. El dolor en la zona afectada se siente más por la noche y esto está relacionado con el pico de cortisol que es una hormona que se produce exclusivamente durante el día, pero no por la noche, ya que se considera inútil para nuestro cuerpo. Esto explica por qué todos los dolores tienden a inflamarse por la noche. Los pacientes que acuden a la clínica -añade el doctor Gianni- por los problemas de los que hemos hablado, por ejemplo el túnel carpiano, o las lesiones por esfuerzos repetitivos, o las parestesias, no son conscientes de cuáles son los desencadenantes de estas patologías, de hecho, en la mayoría de los casos, son totalmente inconscientes de ellas. Esta laguna de conocimientos persiste a pesar de que los medios de comunicación transmiten mucha información sobre la ergonomía, las buenas prácticas y las posiciones que deben adoptarse durante el trabajo o la escuela. Los desencadenantes de ciertas patologías salen cuando el médico empieza a hacer preguntas específicas sobre el comportamiento habitual. Por ejemplo, escribir en el teclado o usar el ratón es la principal causa de los problemas de codo y hombro. Le preguntamos al doctor cómo intervenir en este tipo de patología. En primer lugar, aconseja al Dr. Gianni, una intervención temprana es necesaria. El tratamiento puede ser tanto farmacológico como fisioterapéutico y muchas veces, por desgracia, debe ser quirúrgico. Por ejemplo, hablar del síndrome del túnel carpiano, uno de los más característicos, causado por el uso prolongado del ratón, la escritura fuerte y repetida en el teclado y todas aquellas acciones que estresan el distrito articular de la mano, puede conducir, a la larga, a un síndrome de compresión del nervio mediano que causa parestesias, hormigueo, pérdida de fuerza en los distritos afectados, dolores nocturnos. En las etapas iniciales podemos simplemente hacer una terapia de drogas que por lo general tiene éxito en la eliminación de la inflamación. Normalmente se puede recuperar casi el 100%, si la droga también se apoya en el cambio de hábitos laborales y posturales. Si es necesario, se puede añadir una fisioterapia dedicada, con el uso de medios físicos, que sirve para mejorar y acelerar la curación. Otras veces la lesión está en una etapa tan avanzada que la fisioterapia y la farmacología por sí solas no pueden resolver el problema. En este caso, la cirugía es necesaria. En el caso del túnel carpiano, la operación implica el

desbridamiento del nervio mediano mediante la limpieza del túnel a través de una pequeña incisión. El médico añade entonces algunos consejos, rápidamente, sobre las buenas prácticas que deben adoptarse durante el uso del terminal de vídeo. En primer lugar:

- Realizar descansos durante la actividad, aunque sean pequeños, de uno o dos minutos, repetidos frecuentemente a lo largo del día. Incluso un pequeño paseo por la habitación puede ser suficiente.
- Hacer ejercicios de estiramiento de las extremidades superiores para estirar los músculos extensores y flexores del cuerpo.
- Estirar la columna vertebral, porque una posición sentada, prolongada en el tiempo, provoca una carga excesiva en la columna lumbosacra, que implica, por lo tanto, la parte terminal de la columna que está más comprometida en la posición sentada. Paradójicamente, el síntoma que afecta a la columna vertebral es más evidente en una posición fija que en una actividad, incluso pesada, que no obliga a una inmovilidad prolongada.

En cuanto a la ergonomía de la estación de trabajo, recomendamos una posición correcta del tronco de la columna que forma un ángulo de 90 grados con los miembros inferiores. El escritorio debe estar a una distancia adecuada y cómoda. En muchos casos, sería aconsejable mantener un reposapiés bajo el escritorio para poder descargar los miembros inferiores. Un redescubrimiento moderno son las sillas suecas, que permiten mantener una postura erguida de la columna, porque no tienen respaldo. La postura, a la que obligan, hace que los músculos extensores de la columna trabajen activamente para salvaguardar su estructura. También es importante descansar los codos correctamente, manteniendo el asiento a una distancia correcta del escritorio. Esto es para evitar crear una compresión a nivel del canal cubital, donde el nervio cubital que podría sufrir. El monitor también debe estar correctamente posicionado, determinando un ángulo de visión que permita mantener la cabeza en una posición neutral, ni demasiado flexionada hacia adelante ni demasiado hacia arriba. Cuando se le pregunta si conoce los cursos de ergonomía para las escuelas, el Dr. Ganni responde: "La pregunta, que es muy pertinente, me dio la pista para hablar de una experiencia personal mía. En mi formación, en Francia, me enteré de cursos, para una buena higiene postural, impartidos por las administraciones de grandes empresas, y realizados por médicos especializados en Fisiatría.

Las grandes empresas multinacionales, con un elevado número de empleados que trabajan en las computadoras, prefieren invertir en prevención en lugar de en asistencia. Descuidar la salud de los empleados significa pagar, en todo caso, a los recursos humanos, en licencia por patologías debidas, en este caso, a malos hábitos posturales. Varios estudios estadísticos - agrega el director- señalan una disminución significativa de los períodos de enfermedad y una mejora general de la salud de los empleados que han participado en estos cursos de formación. Crear cursos de ergonomía - añade - sería una cosa a hacer, lo antes posible, también aquí en Italia".

### 3.2.3. Entrevista con el asistente técnico del laboratorio (AT)

La Sra. Addario nos invita a su laboratorio para responder las preguntas de nuestra entrevista. Primero esboza la figura del técnico de laboratorio y las tareas que se le asignan. El papel del asistente técnico se ha introducido en las escuelas italianas desde hace unos 20 años. Su función, que en un principio sólo se refería al mantenimiento de los equipos y programas informáticos que contenía, hoy en día amplía sus prerrogativas a la función de ayudante del profesorado. Específicamente, sus deberes son:

- Preparar y establecer los talleres y dirigirlos en conjunto con el profesor;
- El mantenimiento del equipo y la búsqueda de material
- Establecer un enlace con la oficina técnica en las actividades de coordinación

Los técnicos de laboratorio son las figuras predispuestas a prestar apoyo a los profesores y estudiantes en su intento de aprovechar la enseñanza digitalizada. El horario de trabajo es de 36 horas semanales, de las cuales un máximo de 24 horas semanales con un profesor y el resto para el mantenimiento de los instrumentos. Nos dice que la tarea del asistente técnico comienza en el mismo momento en que un profesor decide preparar una lección con el apoyo de recursos digitales o en línea. El técnico proporciona las herramientas necesarias para llevar a cabo la lección. También ofrece apoyo técnico durante la lección para cualquier dificultad relacionada con el uso del hardware o los diferentes programas informáticos en uso, ayudando tanto a los profesores como a los estudiantes individuales. Por consiguiente, a menudo las intervenciones también conciernen a la organización de la enseñanza porque las asignaturas,

en su opinión, aún no han sido calibradas para ser enseñadas con herramientas informáticas. Le preguntamos si, en su opinión, los alumnos perciben que están tomando riesgos al navegar por Internet. El técnico nos responde directamente: "No, en absoluto". Lo primero que hacen los estudiantes, revela, frente a los ordenadores del laboratorio es ir a sitios prohibidos, duros o redes sociales. Nos preguntamos, por lo tanto, qué tipo de trucos pone la institución escolar para evitar estas imprudentes e indiscriminadas navegaciones. Los ordenadores en uso, admite el técnico, no tienen restricciones en la navegación. Los alumnos son potencialmente libres de entrar en cualquier sitio. El único elemento disuasorio es la posibilidad de que el técnico, a través del ordenador central, equipada con un software de control, pueda visualizar la pantalla de cada estudiante y bloquear su teclado y su ratón, en caso de que descubra que está navegando en un sitio inapropiado.

Sin embargo, este tipo de control no es suficiente para frenar ciertos comportamientos indebidos y, por lo tanto, los profesores y técnicos se ven obligados a pasar entre los pupitres para reforzar el control. Cuando nos referimos a los programas y habilidades de seguridad de los estudiantes, el técnico dice que los estudiantes no son en absoluto conscientes de la existencia de programas para la seguridad de los dispositivos informáticos o que, al menos en el laboratorio, no los utilizan. Nuestras preguntas sobre la capacidad de los estudiantes para proteger su salud del uso excesivo de Internet confirman que los estudiantes no están interesados en la protección de la salud de ninguna manera o tal vez ni siquiera saben que la están poniendo en riesgo. Aunque todos los criterios relativos a la ergonomía, por ejemplo, se han cumplido en la construcción del laboratorio, demuestran que no los conocen. En cuanto a los sistemas de eliminación de los dispositivos informáticos para la protección del medio ambiente, se nos asegura que los alumnos no tienen ningún conocimiento sobre cómo eliminar estos dispositivos y añade que ni siquiera están interesados en ellos y por lo tanto no respetan la recogida selectiva de residuos, que es obligatoria para todos. En lo que respecta a la protección de los datos personales y el riesgo de que sean robados, revela, por otra parte, que ha observado comportamientos para salvaguardar estos últimos. Muchos estudiantes, de hecho, piden al asistente técnico que compruebe el cierre real de su cuenta. También piden que se abran nuevas cuentas y que no se utilicen las cuentas personales para la enseñanza, por temor a que se abran en su ausencia o sin su permiso. Todas las precauciones y precauciones que han aprendido de sus compañeros de clase y que no provienen de la escuela, ni en forma de cursos, ni por parte de profesores o técnicos. Preguntamos si se han establecido sistemas de seguridad para defender los datos personales de los robos. El técnico nos asegura que los

ordenadores individuales están defendidos por un cortafuegos, pero no hay ninguna protección dirigida específicamente a los estudiantes. La única solución es el uso de diferentes cuentas reservadas para estudiantes, profesores y técnicos que también actúan como administradores. En cuanto a la libertad de utilizar el teléfono móvil en el aula, el técnico revela que, aparte de los raros casos en que se les pide que lo utilicen por motivos educativos, existe una prohibición expresa de utilizarlo o dejarlo encendido. Sin embargo, la solicitud se desestima regularmente. Los estudiantes miran constantemente sus teléfonos inteligentes y reciben recordatorios y advertencias, que no son atendidos. Por otro lado, también es difícil para los profesores controlarlos, ya que la estación de trabajo detrás de los ordenadores oculta sus movimientos. Desde el punto de vista de la digitalización, es decir, la presencia de laboratorios modernos con tecnología moderna, la escuela, confirma la Sra. Addario, está bastante en línea con las normas nacionales. Los laboratorios, de hecho, están equipados con máquinas relativamente nuevas y software de vanguardia. En cuanto a la formación digital de los profesores, el técnico nos informa de que es bastante deficiente aunque se hayan realizado cursos de actualización (más o menos válidos), de acuerdo con los requisitos legales. Pudo observar que sólo se seguían los cursos obligatorios, con un interés que en algunos casos se percibía como bajo.

Por otro lado, añade, todo lo que es obligatorio y no de libre elección nunca se hace bien. Preguntémosles, entonces, cuáles son las repercusiones en la enseñanza de estos cursos. El técnico responde: "pocos o ninguno". En general, los profesores no pueden trabajar de forma independiente, siempre necesitan el apoyo del técnico, incluso para los casos que van más allá de las habilidades y obligaciones del técnico de laboratorio individual. Ahora preguntamos al técnico si, desde su punto de vista estratégico, fue capaz de observar si los alumnos están preparados para tratar de forma crítica y responsable la información procedente de la red. En lo que respecta al período de dos años, el técnico es categórico: "No, porque llegan totalmente desprevenidos de la escuela secundaria". Por otra parte, en lo que respecta al período de tres años, sobre todo en lo que se refiere a las clases terminales, pudo observar una actitud diferente por parte de los estudiantes que se acercan a las noticias en línea de manera crítica. Sin embargo, nadie los ha entrenado en este sentido. En este punto le preguntamos al técnico qué porcentaje, en su opinión, usan los maestros el taller. Nos dice que alrededor del 60% de los profesores usan los laboratorios semanalmente, el 40% restante nunca los usan. Sin embargo, todos utilizan el Lim (pizarra multimedia interactiva) que está a su disposición en cada clase. En este caso, después de 3-4 años de cursos, ahora pueden definirse como

autónomos. Los programas didácticos, sin embargo, utilizan una pequeña parte de la computadora y de los recursos en línea porque estos dispositivos se utilizan como herramientas de salida y entrada y no entran más que eso en la didáctica que todavía se sigue entregando de manera clásica. Sin embargo, a esta regla le siguen excepciones, a saber, profesores ultramodernos que prueban su habilidad para impartir lecciones innovadoras con la ayuda de programas informáticos específicos que tienen un gran impacto en los estudiantes. Esta búsqueda de innovación y transformación de los programas de enseñanza no está vinculada a la materia, si pertenece a las disciplinas matemáticas lógicas o humanísticas, sino que se refiere exclusivamente a la disposición del profesor individual a experimentar nuevas formas de enseñanza. El técnico añade que una mayor implicación de las herramientas informáticas en la enseñanza sería sin duda un incentivo para el aprendizaje por parte de los alumnos, pero, tal como están las cosas, ni los profesores ni los alumnos están preparados, ya que demuestran que no perciben Internet como un recurso de aprendizaje, sino como un canal para conectarse a las redes sociales. Por eso se les prohíbe absolutamente el acceso a los talleres en ausencia del maestro o del técnico. Nos preguntamos, una vez más, qué es lo que falta en las instituciones educativas para que puedan hacer un uso rentable y seguro de los dispositivos informáticos. El técnico nos cuenta cómo hace unos años se inició un proyecto experimental en una sola clase que también implicaba la compra de 30 tabletas, una para cada estudiante. Se les pediría a los estudiantes que sustituyeran los libros por la única tableta que se les entregara. Todas las tabletas tendrían instalado un software para trabajar en red incluso desde casa. Desafortunadamente el proyecto nunca comenzó. Tal vez porque a los profesores se les exigía una preparación específica que no tenían, un esfuerzo extra que sobre todo los profesores mayores y cercanos a la jubilación no estaban dispuestos a hacer. Para trabajar en línea, por otro lado, es necesario tener una estructura mental diferente a la clásica de las viejas generaciones. El proyecto no se inició en absoluto y las 30 tabletas fueron entregadas a los profesores para reemplazar varias computadoras que fueron robadas en el mismo año. Los maestros usan estos dispositivos en préstamo desde el principio del año escolar hasta el final, cuando están obligados a devolverlos a la oficina de la secretaria. Nos preguntamos cómo deberían ser los profesores digitalizados del futuro. El técnico nos responde: "Mientras tanto, curioso, abierto a lo nuevo, dispuesto y listo para involucrarse. No deberían ver la digitalización como un monstruo alienígena temible". Entonces el técnico dice que la escuela también debería intervenir más eficazmente, y luego seguir a las autoridades a nivel regional y nacional, comenzando desde abajo hacia arriba, y ya no desde arriba. Incluso si la



mecanografía en la escuela estaba prevista por la Buena Escuela fue, desde este punto de vista, desestimada. Addario afirma que la prioridad de la intervención corresponde a los profesores, que necesitan cursos de formación específicos, profesionalizantes y variados; luego a los alumnos, empezando por los cursos de seguridad en línea. En lo que respecta a los padres, no se pronuncia porque, hasta ahora, no se han involucrado en el tema en absoluto.



## **CAPÍTULO IV**

### **Análisis del contexto escolar**

#### **4.1. Ciclo de la escuela italiana**

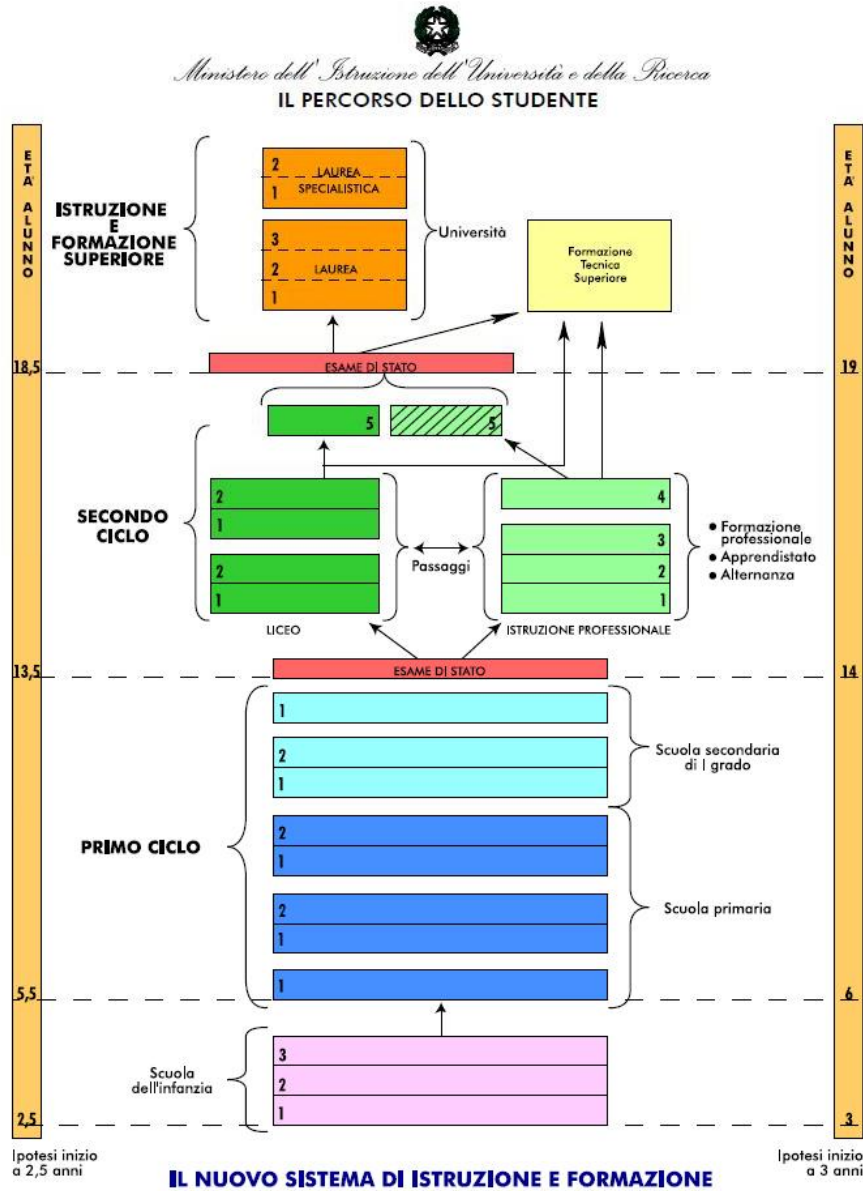
En Italia, el debate entre las escuelas públicas y privadas sigue abierto, con normas y disposiciones que declaran explícitamente que quieren "igualar", asimilar, equiparar la formación privada al Estado, pero con excepciones y laxitudes que hacen que todo cambie para que todo siga igual, parafraseando a Tomasi di Lampedusa (2002). Sin embargo, es necesario discriminar entre las diferentes escuelas definidas como "no estatales". En primer lugar, nació la paridad religiosa, a la que se ha añadido la paridad secular y la no paridad. Estas escuelas no estatales, surgidas en el curso de la historia italiana, han conocido la fortuna en fases alternas, como consecuencia de impulsos económicos, políticos y religiosos a menudo opuestos si no en la práctica, ciertamente en las ideologías. El sistema escolar italiano ha sufrido continuas transformaciones en el escaneo de los ciclos escolares. Hasta la fecha, la trayectoria escolar de cada estudiante sigue el procedimiento descrito en el esquema

publicado en el sitio web del Ministerio de Educación (MIUR) y se estructura de la siguiente manera:

- **Guardería (3 años)**
- **Primer ciclo dividido en:**
  - Escuela primaria (5 años)
  - Escuela secundaria (5 años)
- **Segundo ciclo, escuela secundaria (5 años)**
  - Las escuelas secundarias
  - Educación vocacional
- **Enseñanza superior y capacitación**
  - Grado 3 años
  - Máster de 2 años
  - Formación técnica superior

**Figura 2**

*Diagrama de formación*



Nota. Diagrama tomado de la página web del Ministerio de Educación (MIUR)  
<http://www.miur.gov.it>

## **Preescolar**

Es posible, pero no obligatorio, entrar en el sistema educativo italiano ya a la edad de 3 años o incluso 2.5 para los primeros usuarios (que, sin embargo, se colocan al final del ranking y se insertan solo en las plazas restantes después de la inscripción de los niños de tres años). El curso tiene una duración de tres años, es decir, hasta la finalización del sexto año de edad (5,5 para los que decidan entrar en el primer ciclo como antifipo).

## **Primer ciclo**

El primer ciclo marca el comienzo de la escolaridad obligatoria (que se completará a los dieciséis años). Comprende dos ciclos escolares: la escuela primaria, que dura 5 años escolares (5,5 /6 años hasta 10,5 /11 años); y la escuela secundaria, a la que se accede por simple ascenso y que termina después de 5 años, con la aprobación de un examen de Estado (se extiende de 10,5/11 años hasta 13,5/14 años). Este curso es obligatorio.

## **Segundo ciclo**

El segundo ciclo es una ruta obligatoria hasta los dieciséis años. Para este ciclo se prevén actividades complementarias como el aprendizaje, la formación profesional y la alternancia en la escuela de trabajo. La educación secundaria está dirigida a estudiantes de 13,5/14 años y 18,5/19 años. La escuela secundaria, que termina con la aprobación de un examen de Estado, ofrece dos cursos diferentes:

- Las escuelas secundarias (clásicas, científicas, lingüísticas) consideradas como preparatorias para la universidad y a las que asisten, en teoría, los estudiantes más dispuestos y hábiles que desean completar su educación con un tipo de educación superior;
- Escuelas técnicas o vocacionales, que preparan para entrar en el mundo del trabajo. A pesar de la orientación profesional de estos estudios, no se les impide, sin embargo, entrar en la universidad de la misma manera que los graduados de la escuela secundaria. Aunque en los últimos años algunas facultades universitarias han introducido un sistema de admisión con un número cerrado de estudiantes.

## **La educación superior**

La universidad, en sus diversas ramas y direcciones, se divide en una licenciatura, seguida de una maestría, de 2 años, que permite el acceso a los concursos y a otros puestos de trabajo institucionalizados. La formación técnica superior está destinada a los graduados de institutos profesionales, pero está abierta a todos. Este tipo de formación altamente profesionalizante es impartida por instituciones de formación estatales y regionales.

## **La educación privada y la Iglesia Católica**

En 1929, con el convenio entre el Estado y la Iglesia, se decretó la religión católica como religión de Estado y la enseñanza de la religión católica se hizo obligatoria. El poder de la Iglesia Católica se basaba en la provisión de educación privada, con enseñanzas explícitas de orientación religiosa y la contratación de profesores pertenecientes a órdenes religiosas. Desde 1985, la instrucción religiosa se ha vuelto opcional sólo en las escuelas estatales, donde la Iglesia todavía tiene control sobre el nombramiento de los profesores de instrucción religiosa y la elección de los libros de texto a utilizar. La inspiración religiosa se encuentra en la escuela privada, que se considera una escuela de élite porque está pagada y explícitamente inspirada por los dictados religiosos. Las familias más acomodadas que quieren dar a sus hijos una educación más clásica, una orientación religiosa y un contexto social más protegido y seguro que el de la escuela pública, recurren a los institutos católicos (Ghirardini & Pellinghelli, 2001).

## **4.2. Escuelas privadas laicas**

Además de la educación privada que ofrecen los institutos religiosos, también hay educación de las autoridades locales (municipios y provincias) y de otros particulares de inspiración secular. Los institutos privados seculares más frecuentados parecen ser los institutos secundarios de segundo grado (Baron, 2005). Los nuevos institutos, en general, favorecen y facilitan el proceso de estudio y promoción y, además, prestan otro servicio: la recuperación de los años escolares perdidos. Son escuelas preparatorias que conducen a la admisión en el 5º año. A partir de entonces será obligatorio seguir la ruta del Estado, el único, hasta ahora, capaz de proporcionar un diploma legalmente reconocido. Además de las escuelas privadas,

existen también las escuelas "iguales o "equiparadas" que, asimiladas a las instituciones estatales, deben cumplir ciertas normas de idoneidad, tras lo cual pueden, al final del año escolar, expedir diplomas legalmente reconocidos. De hecho, en 1948, la Constitución italiana estableció que los particulares también podían crear escuelas, sin que ello supusiera una carga para el Estado.

Sobre este punto crucial, es decir, si el Estado concede o no una subvención, todos los debates que aún hoy en día se mantienen vivos giran en torno a las escuelas privadas. A pesar de las numerosas medidas legislativas para que las escuelas privadas sean verdaderamente iguales, en la práctica se ha observado que han podido beneficiarse de "una administración particularmente benévola [...], como lo demuestran el reconocimiento legal otorgado con cierta facilidad y la formación de juntas examinadoras del Estado que son apreciadas por la dirección de las escuelas" (Ventura, 1998). Las escuelas privadas seculares y religiosas en su mayoría toman la dirección opuesta. Los primeros siguen siendo una élite con un programa escolar válido y altamente formativo; los segundos, en cambio, suelen convertirse en un depósito de estudiantes con malos resultados y falta de voluntad para facilitar y acelerar su camino hacia la graduación. Los estudiantes de las escuelas privadas, sean iguales o no, obviamente provienen de familias ricas, es decir, capaces de pagar las caras tasas de matrícula.

#### **4.1.1. Subvenciones y desgravaciones fiscales para las escuelas privadas**

Varios gobiernos han intervenido para apoyar a las escuelas privadas y han legislado a favor de la desgravación fiscal. Estas desgravaciones fiscales se han concedido a los estudiantes menos acomodados que, por necesidad, asisten a escuelas estatales. Estas reducciones están políticamente justificadas por una supuesta igualdad social. Con el tiempo, sin embargo, los alivios también se han concedido a los alumnos que asisten a escuelas no estatales, y por lo tanto por una cuota. Con los decretos ministeriales 261/98 y 279/99 (Ambrosini & Caneva, 2011) se ha llegado a una verdadera financiación de las instituciones no estatales. Con la Ley de Igualdad, N° 62 de 2000 (Marzuoli, 2002), se han desarrollado disposiciones y reglamentos en el sentido favorable al sector privado, al tiempo que se establecen ciertas condiciones que deben cumplir, especialmente las escuelas privadas de igualdad, que a partir de ahora son



bastante distintas de las escuelas simplemente privadas. Las instituciones privadas no estatales se dividen en:

- Instituciones de concertadas en virtud de la Ley 62 de 10 de marzo de 2000;
- Instituciones no unificadoras;
- Los institutos extranjeros, gracias al decreto del Presidente de la República 389 del 18 de abril de 1994 (Parisi, 2011).

Las escuelas iguales pertenecen, de hecho, al sistema nacional. Por esta razón, sus estudiantes están obligados a completar su educación, tienen los mismos derechos y deberes que los estudiantes del Estado, y su curso termina con los exámenes del Estado, que pueden realizarse en la propia institución de ahora en adelante, con los mismos procedimientos que los del Estado.

En cuanto a los estudiantes que asisten a escuelas privadas pero no subvencionadas, podrán completar su escolaridad obligatoria, pero tendrán que tomar los exámenes del Estado en las escuelas públicas para que sus certificados intermedios y finales tengan certificación legal. También tendrán que hacer una prueba de aptitud al final de cada carrera escolar si pretenden pasar a una escuela estatal o igualitaria.

Según el mismo párrafo cuatro de la Ley N° 62 de 2000. Las escuelas capaces de elaborar un proyecto educativo sobre la base y de acuerdo con los dictados de la Constitución italiana, que presentan un plan de la oferta educativa adaptado a las normas y disposiciones vigentes, que certifican la propiedad de la gestión de la escuela y que aceptan la publicación de los estados financieros pueden tener reconocida el concierto.

A esto se añade, sin embargo, la necesidad, por parte de los solicitantes, de disponer para la construcción de la escuela y para la preparación de las clases individuales:

- Aulas adecuadas para fines educativos;
- Muebles y herramientas didácticas (según lo dispuesto en el reglamento de las escuelas estatales);
- Órganos colegiados que toman decisiones de manera democrática;
- La inscripción está abierta a todos los alumnos con una calificación válida o que presenten un certificado de promoción del año anterior al solicitado.

También será necesario que la escuela garantice:

- Medidas disuasorias y compensatorias para los alumnos con discapacidades o necesidades educativas especiales, adaptadas a su condición y que les permitan asistir a la escuela, como exige la legislación vigente;
- El establecimiento de cursos completos o la finalización de los que acaban de empezar;
- Los profesores están calificados para enseñar;
- Los contratos de trabajo individuales respetan los límites impuestos por el contrato nacional aplicado al sector escolar (Astorri, R., 2000).

Todas estas garantías autocertificadas serán, en un primer momento, objeto de evaluación por parte del sistema nacional y deberán respetar los dictados de la normativa vigente. De acuerdo con la Constitución, también pueden hacer uso de los servicios voluntarios de los propios profesores, siempre que la actividad no supere la cuarta parte del total de los servicios prestados.

En el mismo párrafo se especifica que el Ministerio de Educación será el órgano encargado de comprobar la veracidad de las declaraciones y la posesión de los requisitos declarados para obtener la igualdad y la permanencia de estos requisitos en el tiempo (Astorri, R., 2000).

Por su parte, la Oficina Escolar Regional preparará los controles y reconocerá la condición de igualdad para cada institución solicitante. Sin embargo, por experiencia personal, creo que estas comprobaciones se realizan de manera bastante deficiente e imprecisa. En algunos casos fue el propio Ministerio de Educación el que confirmó la hipótesis de una aplicación sumaria y reducida de la normativa por parte de las escuelas privadas (Barón, 2005). Este fenómeno fue posible gracias a la obtención de certificados de paridad mediante una simple autodeclaración de la escuela, que, sin embargo, no fue seguida de los controles previstos y necesarios.

El Ministerio, añade el Barón, confirma que está al tanto de las actividades educativas que no cumplen con los reglamentos escolares o las obligaciones legales y reglamentarias. De hecho, los alumnos suelen recibir un trato demasiado benévolo, como la posibilidad de inscribirse

directamente en el último año del curso elegido y de presentarse a los exámenes de las juntas examinadoras, que son demasiado indulgentes. (Barón, 2005).

La escuela privada tiene otros privilegios en virtud del decreto de aplicación de la Ley de finanzas de 2003 (Freni, 2003). El decreto prevé, de hecho, contribuciones financieras en forma de reembolso de los gastos de escolaridad. Sin embargo, estas contribuciones no se conceden a las escuelas estatales.

En virtud de la Ley de finanzas de 2003, la asignación de las bonificaciones económicas en cuestión ya no está vinculada, inexplicablemente, a los ingresos familiares. Habría justificado, al menos moralmente, su concesión exclusiva a las familias menos acomodadas, al menos moralmente, su concesión exclusiva a las escuelas privadas.

Con el presupuesto de 2007, continúan las disposiciones en favor de las escuelas privadas. De hecho, se define la cantidad de contribuciones asignadas a las escuelas iguales. Esto se dispuso en el decreto anual del Ministro de Educación, Universidad e Investigación, de conformidad con el párrafo 636 del artículo 1 de la Ley 296 de 27 de diciembre de 2006.

#### El Plan de la “Buona Scuola”

En 2015 se introdujo el plan de la Buena Escuela (Nocera, S. & Tagliani, N. 2015). También en este caso el Ministerio de Educación ha previsto un favoritismo en relación con las escuelas privadas, pero también ha preparado un plan extraordinario de inspección, para garantizar la calidad del proceso de formación que ofrecen las escuelas de igualdad.

Con esta determinación, el gobierno ha expresado la intención específica de eliminar a los llamados diplomáticos y recompensar a las escuelas iguales que, en cambio, trabajan de manera virtuosa.

El plan de la Buena Escuela, con un plazo de tres años, ha revisado, de manera particular, la situación de las escuelas secundarias subvencionadas. Con ese fin, se ha creado un grupo de coordinación junto con las Oficinas Escolares Regionales y se ha duplicado el número de inspectores, pasando de 56 a 104. El objetivo de esta acción gubernamental es verificar los requisitos que poseen las distintas escuelas para acceder y mantener la igualdad adquirida. En el primer semestre de 2016, se inspeccionaron 288 escuelas, de las cuales sólo se ha retirado

la subvención a 27. Para dar cuenta, las principales críticas que se encontraron durante las inspecciones en las instituciones de subvencionadas se referían a los siguientes aspectos:

- Documentación de seguridad defectuosa;
- El local no es adecuado para el servicio escolar;
- El plan de oferta de entrenamiento incorrectamente completado;
- La diferencia entre el número de alumnos matriculados y el número de alumnos que realmente asisten.

Las intervenciones tuvieron lugar principalmente durante los exámenes preliminares, de idoneidad y de estado.

Sólo el anuncio del inicio del Plan de Inspección ha reducido el número de inscripciones de 5.963 en 2015 a 5.168 en 2016, (-13%) (Magni, 2016).

Conscientes de esta realidad tan extendida en Sicilia y, en particular, en la provincia de Ragusa, hemos elegido para nuestra encuesta comparar un instituto estatal y otro privado, ambos de Vittoria en la provincia de Ragusa.

#### **4.1.2. Contexto económico y social en la ciudad de Victoria**

Los dos institutos investigados se encuentran en el mismo municipio: Victoria. La ciudad, de unos 60.000 habitantes, es un gran centro agrícola y comercial situado en la provincia de Ragusa. La ciudad, fundada en 1607, está situada en una gran zona plana, a unos pocos metros (70 m) sobre el nivel del mar.

La ciudad tiene una estructura moderna de tablero de damas con calles anchas y rectas. El clima y la vegetación son típicos del maquis mediterráneo. La baja altitud de la llanura de Victoria, determina temperaturas medias más cálidas que las registradas en el resto del territorio de las montañas de Iblei. Gracias al factor climático, el área territorial es rica en actividades en los sectores:

- Agricultura (con cultivo en invernadero de tomates y primeros frutos);
- Floricultura (con la absoluta primacía de los claveles);

- Viticultura (con la producción de uvas de mesa y vinos de mezcla de alta calidad como el vino D.O.C. "Cerasuolo di Vittoria");
- Comercio (con uvas, huevos, verduras);
- Cría de ovejas y ganado;
- Pesca (en el puerto pesquero de Scoglitti).

Su economía combina la producción y el procesamiento de recursos agrícolas con el desarrollo del turismo, el comercio y la industria (procesamiento de productos agrícolas). Hoy en día Victoria goza de un alto nivel económico y un buen número de turistas.

El sector secundario parece seguir siendo escaso (de hecho, la industria metalúrgica acaba de surgir) y el sector de los servicios sigue creciendo. Estos sectores, que siguen creciendo, necesitan figuras especializadas que deberían dejar la enseñanza obligatoria.

Las escuelas profesionales o técnicas, como las que estamos estudiando, trabajan de hecho para formar y desarrollar las habilidades empresariales de sus estudiantes, con la esperanza de que estas habilidades, a su debido tiempo, se gasten en la misma área.

Según datos del ISTAT, al 31 de diciembre de 2018, la población extranjera residente es de 7.192 habitantes. Las minorías más representadas son los rumanos y los tunecinos. Se emplean en trabajos pesados, especialmente en invernaderos, con ritmos de trabajo a menudo agotadores y mal pagados. Casi siempre es un trabajo ilegal.

Además del italiano en Victoria, así como en la mayor parte de Sicilia, el dialecto siciliano se habla en su variante sudeste. Los estudiantes sicilianos, junto con los estudiantes extranjeros, practican constantemente la lengua italiana sólo desde la escuela obligatoria. Las excepciones son los estudiantes de clase media o media alta que aprenden a hablar italiano con fluidez en casa a una edad temprana con sus padres, a menudo graduados. Estos estudiantes, sin embargo, generalmente no se matriculan en escuelas técnicas (como las que hemos elegido para esta investigación), sino en escuelas secundarias.

La integración con el territorio se ve favorecida por la interacción entre la escuela, las autoridades locales, la Iglesia y las asociaciones culturales que operan en el territorio. La filosofía que guía las elecciones educativas, administrativas y sociales es la de una Escuela

que representa un punto de referencia y agregación. Un sujeto activo capaz de promover la cultura y la integración en el territorio.

Al igual que en los niveles inferiores de educación (escuelas primarias y secundarias), los programas educativos de ambas instituciones que se están examinando incluyen herramientas para la integración y la inclusión. De hecho, hay numerosos proyectos aprobados por el Ministerio del Interior para la integración de nacionales de terceros países. Las estrategias de inclusión e integración y también las técnicas de recuperación lingüística, creadas para alumnos extranjeros, se proponen también a alumnos procedentes de realidades sociales difíciles.

La verdadera emergencia en Sicilia, sin embargo, en mi opinión, no es la presencia masiva de migrantes, sino la gestión empresarial de la Escuela. En los últimos años, los directores de las escuelas se han convertido en pequeños empresarios que responden a las leyes económicas y no al valor superior de la cultura y la formación. Los resultados están bajo los ojos de todos, como confirman los datos de los informes Invalsi de los últimos años. Estas encuestas, de hecho, apuntan a una escuela que todavía es vieja, no está preparada y es desorganizada, no es capaz de preparar a los alumnos para la comparación con las generaciones europeas. La preparación de los estudiantes sicilianos es, de hecho, mucho más baja, no sólo que la alcanzada por los estudiantes de otros países europeos, sino también en comparación con el propio norte de Italia.

Ciertamente no todas las responsabilidades pueden ser atribuidas a la Escuela. En la evaluación de esta distancia cultural entre los jóvenes europeos, en detrimento de los estudiantes sicilianos, debe reconocerse el papel del contexto cultural y social de las familias a las que pertenecen como atenuante y al mismo tiempo agravante.

En una realidad en la que la mayoría de los adultos todavía hablan el dialecto; en la que todos los abuelos y unos pocos padres, todavía están vinculados a las actividades de trabajo manual; en un lugar en el que la cultura sólo era un obstáculo para las familias porque perdieron las armas de trabajo indispensables para la supervivencia. En una realidad en la que todos los sacrificios nunca han llevado a la elevación social. En un lugar, como este, donde la esperanza de un futuro mejor que debe ser conquistado a través de la educación todavía choca con una realidad dada, donde el mérito casi no existe. En este lugar nacieron los estudiantes sicilianos

de los Institutos Fermi y Verga, cuyas habilidades son objeto, en esta tesis, de nuestra evaluación.

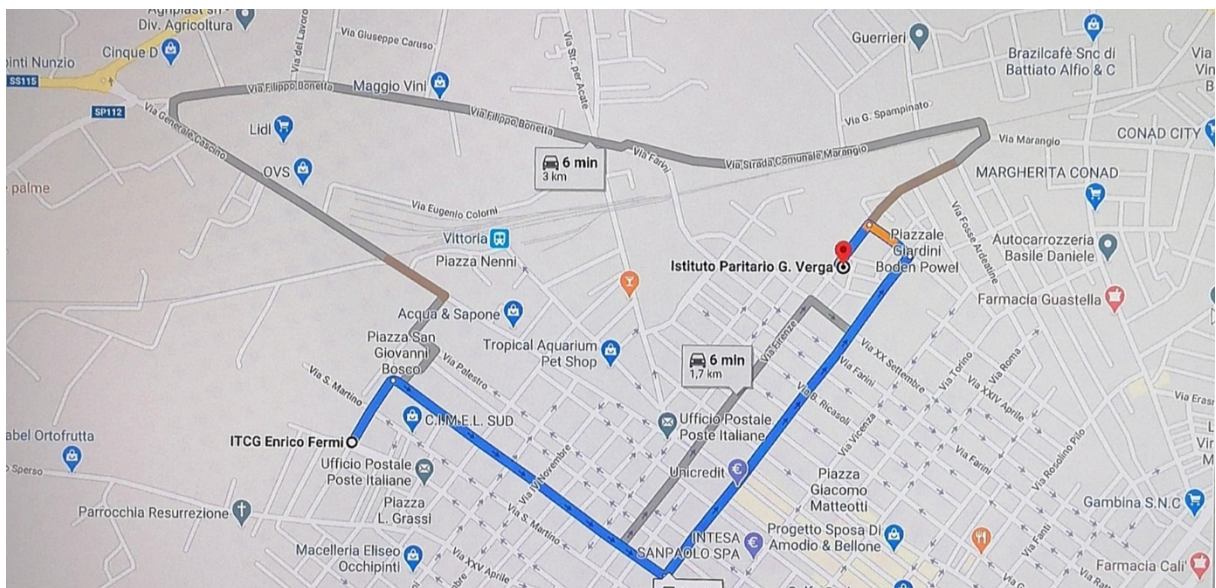
**Figura 3**

*Ubicación geográfica de las escuelas. De Google Maps*



**Figura 4**

*Recorrido de una institución a otra*



#### **4.1.2. El instituto público**

El Instituto Estatal E.Fermi, situado en Vittoria, comenzó a funcionar en el sector escolar en 1970. Desde su creación, el instituto ha representado un punto de referencia profesional, cultural y social para la ciudad. Los programas innovadores y la experimentación de vanguardia han mejorado significativamente la calidad de la educación y la vida asociada para los estudiantes, los padres, los maestros y el personal de la escuela. A partir del año escolar 2014-15, como parte del plan de dimensionamiento de las escuelas secundarias de la provincia de Ragusa, el Instituto ha agregado el ITA, ofreciendo así 3 cursos de estudio:

- Sistemas de Información Corporativa;
- Construcción Medio Ambiente y Territorio;
- Sección de Agricultura - Agroindustria - Agroalimentación.

El Instituto fue fundado alrededor de los años 70 como una rama del ITCG de Ragusa. Su institución está vinculada a la necesidad de contar con institutos técnicos en la provincia de Ragusa que puedan responder a las solicitudes de una base de usuarios en continua expansión.

En el año escolar 1970/71 las clases se convirtieron en 14 con 316 alumnos y 32 profesores. La sección comercial incluía ocho clases, mientras que seis clases conformaban la sección de Geómetras. En los siguientes años escolares, hasta 1974, las clases aumentaron considerablemente, de catorce a dieciocho, y luego veinticuatro (13 clases en la sección comercial; 11 en la sección de agrimensores) en el siguiente año escolar. El Instituto Fermi siempre se ha propuesto como una escuela abierta a nuevas formas de enseñanza, caracterizada por metodologías innovadoras.

La escuela siempre se ha destacado por la elección de un camino didáctico que, además de las herramientas tradicionales, utiliza medios tecnológicos modernos para iniciar a los alumnos en la adquisición de una educación cultural plenamente conectada con el mundo que les rodea.

El Instituto, donde la tecnología tiene un gran espacio, tiene muchos laboratorios a su disposición: Lenguas, Química, Física, Meristemología. Esto le da a los estudiantes una gran



oportunidad de familiarizarse con las computadoras y el software. Algunos programas se dedican principalmente al estudio de la Internet de las redes sociales más comunes: Facebook, Twitter, Badoo.

La escuela se experimenta como la fuerza motriz de la vida asociada, sensible a las nuevas fuerzas motrices y fiel, al mismo tiempo, a las tradiciones de enseñanza validadas por décadas de experiencia. El Instituto también está acreditado como CENTRO DE PRUEBAS para los exámenes de la ECDL para licencias de computadoras, tanto a nivel básico como avanzado.

Desde hace años también se dedica a la realización de proyectos de dimensión y perspectiva europeas: intercambios culturales, pasantías de formación y estancias de estudio en el extranjero. La escuela cuenta con personal especializado en la capacitación en materia de nuevas tecnologías (TIC), en particular para la formación de profesores en el uso de la pizarra interactiva.

La escuela está equipada con varias estructuras de apoyo a la enseñanza:

- Cinco laboratorios informáticos tecnológicamente avanzados;
- Tres laboratorios de idiomas (1 para el período de dos años, 1 para los tres años SIA y CAT, 1 para la sección agrícola, una sala de dibujo (con tecnología informática y computacional) + CAD;
- Un auditorio también preparado para espectáculos teatrales, actividades recreativas y culturales;
- Una biblioteca
- Una sala de reuniones de profesores;
- Un aula audiovisual con conexión vía satélite;
- Un gimnasio;
- Un laboratorio de química;
- Un laboratorio de física;
- Un laboratorio de topografía;
- Un laboratorio con instrumentos para probar materiales de construcción;
- Un laboratorio de meristemología Red escolar del Instituto con conexión rápida a Internet

- Cuatro estaciones multimedia personalizadas para uso exclusivo de los profesores;
- Dos monitores de 40" (para comunicaciones generales en tiempo real).

El Instituto acoge a 950 estudiantes divididos entre la oficina central y la oficina secundaria que alberga los cursos de agricultura, alimentación y agroindustria.

Profesores permanentes: 88,6%.	El Instituto Fermi garantiza un nivel significativo de estabilidad en su personal docente, la gran mayoría de los cuales son profesores titulares. Estos tienen una larga experiencia en la enseñanza y han sido parte del personal de la escuela por más del 50% del personal de la escuela por lo menos 5 años.
Conferenciantes temporales: 11,4%.	
Profesores graduados 91,3%; Profesores graduados 8,7%.	
Maestros de grupos de edad: -...de menos de 35 años de edad, el 1,3%; -35 a 44 años de edad 10,3%; -45 a 55 años 35,9%; -Más de 55 años, 52,6%.	

Características de los maestros (2014-2015) Datos de la RAV. Número total de profesores: 100.

### **4.1.3. El instituto concertado**

El Istituto Scolastico Giovanni Verga opera en el sector escolar desde 1973. La oferta educativa gira en torno a las necesidades económicas del territorio. Los cursos se dirigen principalmente a los jóvenes que quieren recuperar los años escolares perdidos en la escuela estatal. Sicilia, por desgracia, mantiene el triste récord de abandono escolar en comparación con otras regiones italianas. Los alumnos rechazados por las escuelas estatales o que han abandonado la escuela con la esperanza de entrar en el mundo del trabajo y se han visto decepcionados, intentan volver al ciclo escolar y recuperar los años escolares perdidos. Con este fin, las escuelas subvencionadas ofrecen cursos para compensar varios años escolares (a veces hasta tres años) en un solo año. Los estudiantes se matriculan en el último año del curso elegido y durante el año también reciben lecciones de años anteriores en previsión de los exámenes de calificación que tendrán lugar poco antes del examen de Estado. Generalmente los estudiantes aprueban los exámenes de calificación, tal vez, también, porque los exámenes vienen de los profesores que los han preparado teóricamente. Para los exámenes estatales la situación es un poco diferente porque existe la obligación de un comisionado externo.

En 2004, el Instituto G. Verga se ha trasladado a una nueva ubicación y disfruta de instalaciones modernas, grandes espacios, una rica biblioteca, un laboratorio químico y una sala de ordenadores que cumplen con los más altos estándares y por esta razón disfruta de la certificación UNI EN ISO 9001:2000 emitida por el Instituto de Certificación de Calidad "CERTIQUALITY" certificado no. 1264.

Desde 2008 el Instituto Escolástico Giovanni Verga ha adquirido la subvención para:

- Escuela Secundaria Psicopedagógica;
- Sistemas de Información Corporativa;
- Construcción Medio Ambiente y Territorio;
- Sección Agrícola - Agroindustrial - Agroalimentaria.

Las nuevas orientaciones surgen en previsión de las posibilidades de empleo en el territorio y en esta visión han surgido, en los últimos años, nuevos rumbos como:

- Instituto profesional de servicios sociales y de salud. Este es un curso de estudios que dura 5 años. Al final del curso se otorga un diploma de bachillerato, que permite el acceso a cualquier facultad universitaria italiana y extranjera. Un diploma con el mismo valor que los obtenidos en la escuela secundaria estatal. De hecho, se puede acceder a él directamente desde el tercer grado. El programa combina las asignaturas básicas: Matemáticas, italiano, inglés, historia con otras más específicas del sector como: Higiene, Cultura Médica y de la Salud, Psicología, Derecho y Legislación Social y Sanitaria. Las salidas profesionales conciernen tanto a la profesión independiente como a la de asistente de cuidados a domicilio para los ancianos, como al papel de empleado en instalaciones públicas y privadas, como hospitales, guarderías, residencias de ancianos;
- Cursos profesionales para esteticistas cualificados o especializados. El primer curso de estudios incluye la asistencia obligatoria a un curso de dos años acreditado por la Región a la que pertenece. Este curso prevé la concesión de un título, pero no un diploma legalmente reconocido para entrar en las universidades. El segundo, en cambio, prevé tres años de formación, pero los especialistas no estarán obligados a trabajar como empleados, sino que podrán abrir su propia estructura y operar de forma independiente en el sector. El diploma con un examen final sigue siendo insuficiente para matricularse en las universidades;
- Curso para peluquero y peluquero. Este curso incluye la asistencia de dos años de curso con asignaturas teóricas como química y la asistencia a prácticas obligatorias.

La escuela se experimenta como un lugar de encuentro entre estudiantes registrados y no registrados. La formación didáctica se confía a profesores cualificados pero, a veces, sólo a graduados.

La escuela está equipada con varias estructuras de apoyo para la enseñanza:

- Un laboratorio de computación
- Un laboratorio de química;
- Una biblioteca;
- Una sala de reuniones de profesores;
- Un aula audiovisual.

Sin embargo, el número de estudiantes matriculados en las Escuelas de la red privada es modesto en comparación con sus homólogos de la red pública. Las clases alcanzan el número mínimo con dificultad y en ocasiones gracias a inscripciones ficticias

Profesores permanentes: ninguno	El Instituto no puede garantizar la estabilidad de su personal docente. Cada año, según el instituto o el ranking nacional, se contratan diferentes profesores. Pocos están incluidos en el personal de la escuela por más de 2 años.
Profesores graduados temporales: todos ellos.  Profesores graduados: ninguno. No hay un profesor técnico práctico. La única figura que puede enseñar con sólo un diploma.	
Los grupos de edad de los profesores: muy jóvenes, por lo general recién graduados.	



## **CAPÍTULO V**

### **Diseño metodológico del estudio de campo**

#### **5.1. Estrategias de aplicación de los instrumentos**

El modelo utilizado para la creación del cuestionario, como ya se ha indicado, es la Evaluación de la Competencia Digital (Calvani et al., 2014; Calvani, Fini, & Ranieri, 2011; Calvani, Ranieri, & Fini, 2010). Integra cuestiones de carácter puramente técnico con otras de carácter ético-social y crítico-cognitivo, así como otros marcos utilizados en Europa (Calvani & Menichetti, 2014). Esta investigación, sin embargo, se referirá a la competencia digital entendiéndola en el único sentido de la seguridad de navegación en línea. El tema se tratará bajo los aspectos tecnológicos, éticos, cognitivos y de colaboración con la intención de investigar la capacidad de:

1. "Explorar nuevos contextos tecnológicos y enfrentar diferentes situaciones tecnológicas de manera flexible";

2. "Interactuar utilizando las ITC de forma consciente (derechos, deberes, diversidad, normas, riesgos de la red);
3. "Analizar la información, seleccionar, evaluar. Utilizar las tecnologías para la representación y la solución de problemas";
4. "Comprensión del potencial de las tecnologías para la construcción colaborativa del conocimiento (sentido emocional o cívico)" (Calvani & Menichetti, 2014).

La versión completa del cuestionario que administramos, incluye ítems de la escuela de primer y segundo grado relacionados con la seguridad en línea. El cuestionario consta de 40 preguntas divididas en áreas. Las pruebas de seguridad se dividirán en 4 subcategorías:

1. Protección de los dispositivos informáticos (7 preguntas)
2. Protección de los datos personales (9 preguntas)
3. Protección del medio ambiente (4 preguntas)
4. Protección de la salud (6 preguntas)

Estudios de casos (10 preguntas)

Datos personales y opiniones (3+1)

A esta primera sección de preguntas, destinada a evaluar la capacidad de los estudiantes para navegar con seguridad, le sigue una segunda parte destinada a recoger información sociodemográfica de la muestra examinada. Para ello se les pidió que indicaran:

- Edad;
- Clase a la que asiste;
- Horas diarias empleadas en Internet;
- Percibe sensación de riesgo en Internet;
- Opiniones personales sobre los temas tratados.

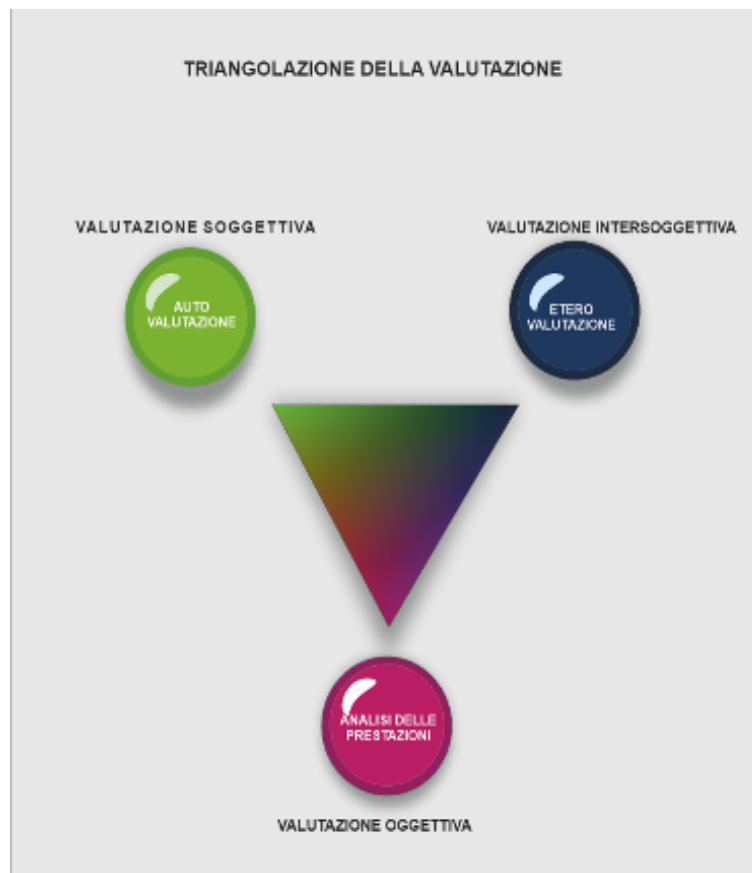
El método adoptado para llevar a cabo esta encuesta es un método mixto, que consiste en entrevistas y cuestionarios estructurados y semiestructurados. Se obtuvieron datos cualitativos de las entrevistas, a los que se añadieron datos cuantitativos de los cuestionarios. La



complejidad de la competencia investigada requiere activar y combinar varias perspectivas de análisis, capaces, en su complementariedad, de darnos una imagen completa del nivel alcanzado por el sujeto. El principio metodológico subyacente es el de la triangulación (Castoldi, 2010), típico de las metodologías cualitativas (ver Figura 5 y 6).

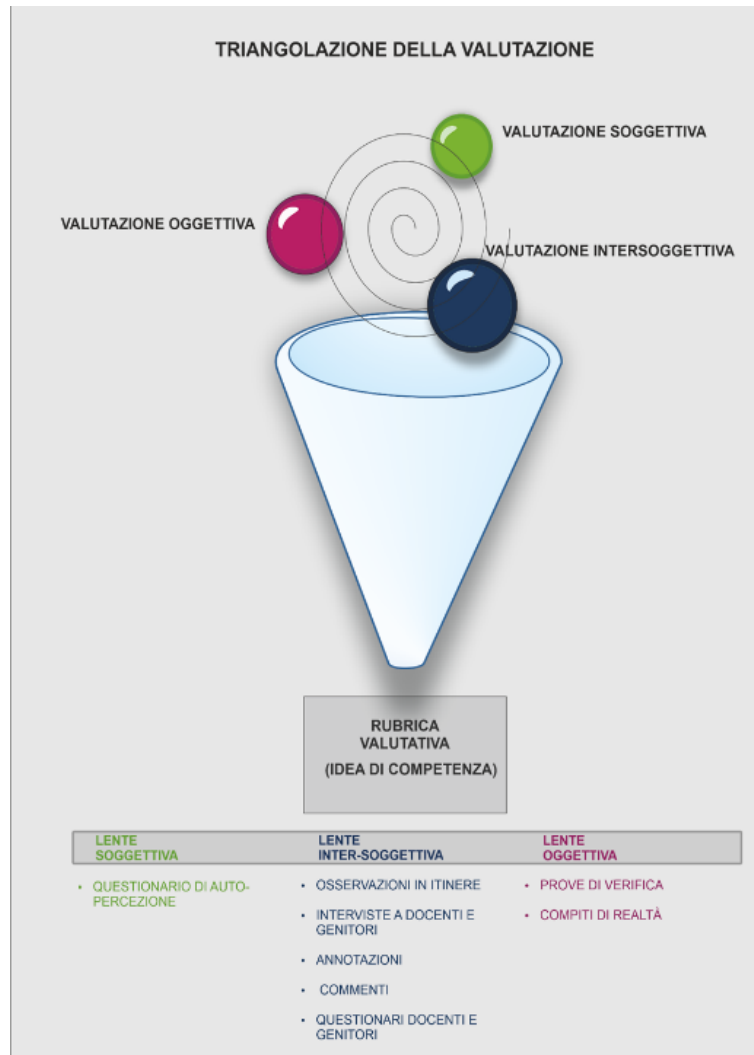
## Figura 5

*Triangulación de la evaluación*



**Figura 6**

*La competencia investigada requiere activar y combinar varias perspectivas de análisis, capaces, en su complementariedad, de darnos una imagen completa del nivel alcanzado por el sujeto*

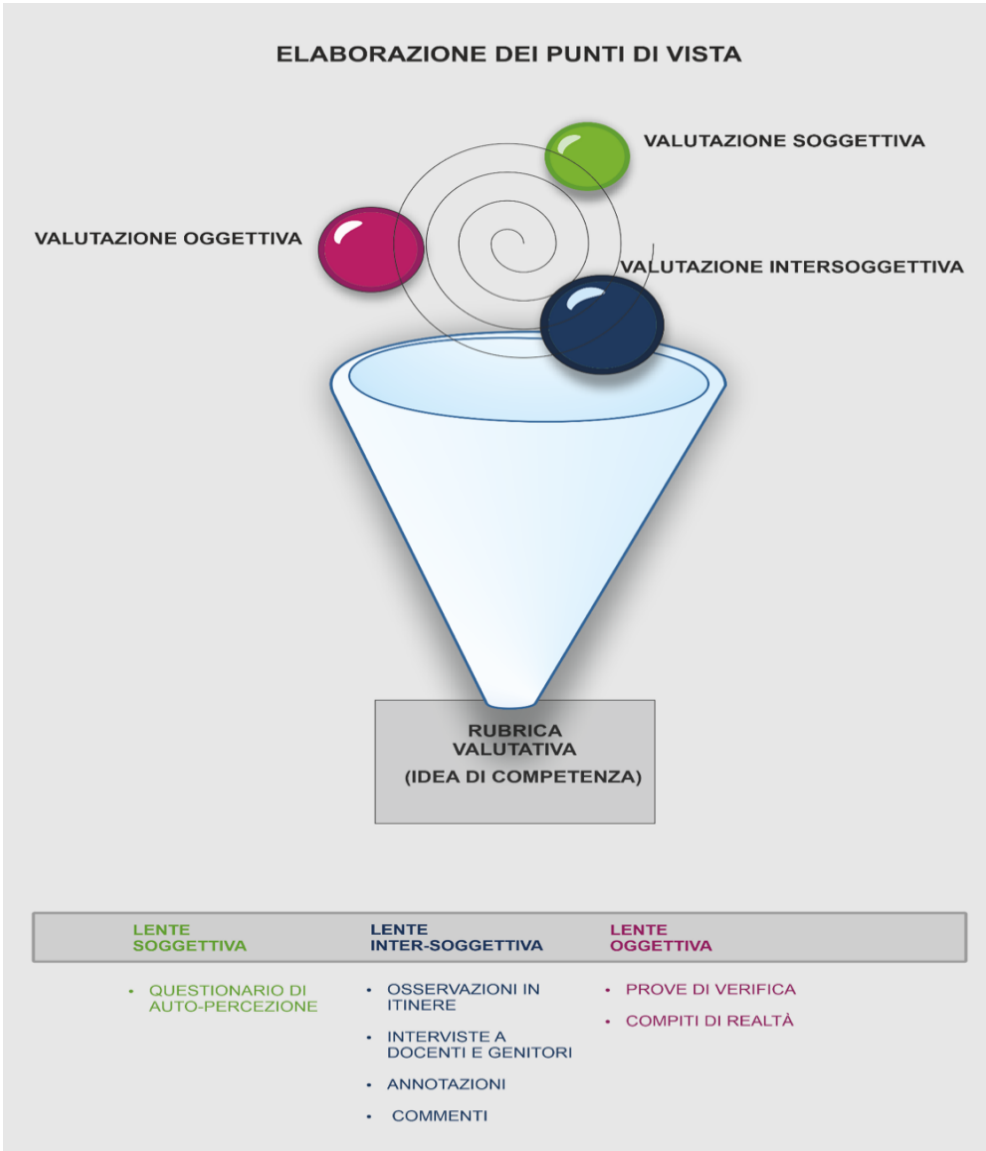


Hay dos escuelas sujetas a análisis: una escuela estatal y una escuela privada y con los mismos cursos de estudios (Técnico Comercial de Administración de Finanzas y Marketing). Ambas escuelas están situadas en el mismo municipio, en la provincia de Ragusa (Sicilia) y no hay otras con la misma dirección. La comparación entre los dos Institutos, estatal y privado, se considera otro punto fuerte a partir de un proceso de comparación sistemática

entre las diferentes perspectivas y la búsqueda de similitudes y diferencias sobre las que estructurar el proceso de interpretación.

**Figura 7**

*Elaboración del punto de vista*



## Figura 8

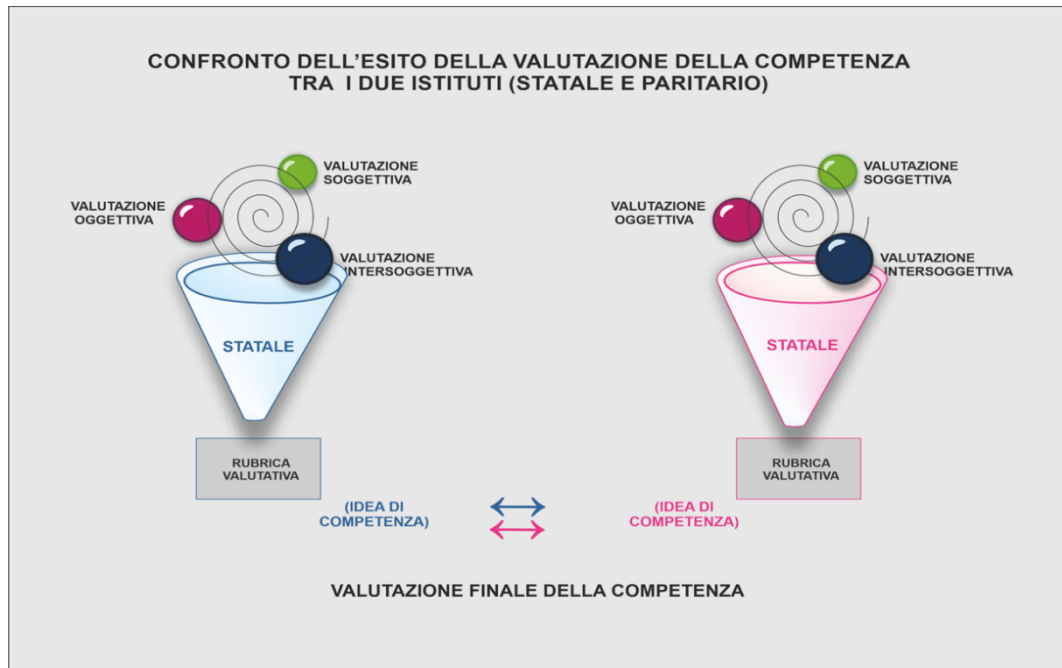
*Escuela estatal y una escuela parificada, con el mismo curso de estudios (Técnico Comercial de administración de finanzas y marketing). Ambas escuelas están situadas en el mismo municipio, en la provincia de Ragusa (Sicilia) y no hay otras con la misma dirección*



La administración del cuestionario se acompañó de otras dos encuestas realizadas con otros tantos cuestionarios rellenos por padres y profesores; a fin de validar su contenido con una triangulación de la evaluación (ver Figura 7). Las tres dimensiones requieren que se integren y compongan diferentes instrumentos. Para ello, en el caso de los profesores y los padres, cuya perspectiva se relaciona con la evaluación intersubjetiva, se utilizaron criterios de observación estructurados y no estructurados como cuestionarios, con preguntas abiertas y cerradas, destinadas a detectar la percepción del fenómeno por parte de los diferentes sujetos, respectivamente los profesores y los padres de los alumnos cuya competencia se iba a investigar (ver Figura 8).

**Figura 9**

*Comparación de las dos triangulaciones aplicadas en las dos instituciones*



Algunas preguntas requieren sólo una respuesta correcta, otras más de una. El número de respuestas necesarias se especifica siempre al final de cada pregunta. La prueba se hizo individualmente en las aulas de clase. Como se acordó con el director después de la entrega del cuestionario, se dieron todas las respuestas correctas, y se realizó una lluvia de ideas con todos los estudiantes en el aula. En cuanto a la participación, tanto el instituto público como el privado, a través de las figuras de los respectivos equipos directivos, acogieron con entusiasmo la propuesta de participar en esta encuesta.

### **5.1.1. Tratamiento de datos**

Durante el tratamiento del cuestionario se determinaron los valores cuantitativos de la encuesta, así como la exhaustividad y la no redundancia de las unidades detectadas y los valores cualitativos, además de las lagunas o los errores de compilación. Un aspecto crucial del cuestionario se refería al "tratamiento de la falta de respuesta (valor faltante), debido a quienes no proporcionan (parcial o totalmente) respuestas al cuestionario" (Signore, Carbini,

D'Orazio, Brancato, & Simeoni, 2010). El término falta o falta de respuesta (no response) se refiere a una multitud de situaciones en las que no se observan los datos. De hecho, se habla de falta de respuesta cuando no es posible obtener los datos de una o más variables de interés para una o más unidades de muestra. Las causas de la falta de respuesta:

- Un aumento de la variabilidad de los estimadores, debido a la reducción de la base de muestras de análisis y/o la aplicación de métodos para su tratamiento;
- Tanto a los estimadores distorsionados, si los encuestados difieren sistemáticamente de los no encuestados con respecto a ciertas características de interés.

Principalmente distinguimos "dos tipos de falta de respuesta, la falta de respuesta total (Falta de respuesta de la unidad) y la falta de respuesta parcial (Falta de respuesta del artículo), que intentamos tratar y resolver aquí". (Bocci, Muratore, Signore, & Tagliacozzo, 2002). Los casos con valores perdidos son un gran desafío porque los procedimientos típicos de modelización no tienen en cuenta estos casos en el análisis "(esto ocurre cuando los valores perdidos son alrededor de menos del 5% del total de los casos y estos valores pueden considerarse como perdidos de forma aleatoria). (Bocci y otros, 2002). Las metodologías utilizadas para tratar la falta de respuesta son diferentes, pero antes de describir lo que se pretende hacer en esta esfera será útil conocer el grado de falta de respuesta de cada variable. Para ello ha sido posible, a través del software SPSS, obtener estadísticas univariadas para las 6 trayectorias de registro que permiten identificar la medida general de los datos que faltan. Para cada variable se ha mostrado lo siguiente en la salida:

- Número de valores no perdidos;
- Número y porcentaje de los valores que faltan.

Además, la media, la desviación típica y el número de valores extremadamente altos o bajos se muestran para las variables cuantitativas (escala). Esta información se ha omitido porque la mayoría de las variables son ordinales y las estadísticas relacionadas se comentarán y discutirán más adelante. En el formato de registro relativo a los padres de los alumnos del instituto técnico-comercial estatal, faltan 4 respuestas relativas a los datos personales "Edad", ya que los sujetos confundieron la pregunta sobre la edad, creyendo que se requería la del niño / alumno y todavía faltan tres respuestas en una pregunta de opción múltiple.

**Tabla 3**

*Resumen de los valores que faltan en el registro de los padres de los alumnos del instituto estatal "X"*

	N	Missing	
		Count	Percent
Età	31	4	11,4
Rischio	35	0	0
Libertà	35	0	0
Tempistica	35	0	0
Sicurezza	35	0	0
Utilizzo_sicurezza	35	0	0
Protezione salute	35	0	0
Sistemi_smaltim	35	0	0
pratica_smaltim	32	3	8,6
furto_dati_person	35	0	0
Salvaguardia dati	35	0	0
Sesso	35	0	0

**Tabla 4**

*Resumen de los valores perdidos en el registro de los profesores de los alumnos del instituto público "X"*

	N	Missing	
		Count	Percent
Età	20	1	4,8
Rischio	20	1	4,8
Libertà	21	0	,0
Tempistica	21	0	,0
Sicurezza	21	0	,0
Utilizzo_sicurezza	20	1	4,8
Protezione salute	21	0	,0
sistemi_smaltim	21	0	,0
pratica_smaltim	20	1	4,8
furto_dati_person	21	0	,0
Salvaguardia dati	21	0	,0
Sesso	21	0	,0



En el registro de los profesores del instituto estatal faltan 5 respuestas en total, una de las cuales está relacionada con los datos personales “Edad”.

**Tabla 5**

*Resumen de valores faltantes en la distribución de registros de los estudiantes de la escuela integral estatal "X"*

	N	Missing	
		Count	Perce nt
Antivirus	84	1	1,2
Virus	85	0	0
Cattivo_consiglio	80	5	5,9
Aggiornamento_PC	79	6	7,1
Antivirus_aggiornato	84	1	1,2
Antivirus_preinstallato	80	5	5,9
Password	85	0	0
Rischi_informatici	80	5	5,9
Pubblicazione_contenuti	84	1	1,2
Accesso_PC_pubblici	81	4	4,7
Cyberbullismo	84	1	1,2
Malware	67	18	21,2
Social_network	84	1	1,2

Social_network2	55	30	35,3
Icona_Mozilla	76	9	10,6
Ricorda_password	85	0	0
Phishing	56	29	34,1
Tre_R	77	8	9,4
Periscoposità_dispositivi	76	9	10,6
Ewaste	58	27	31,8
Gestione_rifiuti	80	5	5,9
Problema_salute_uno	80	5	5,9
Problema_salute_due	82	3	3,5

	N	Missing	
		Count	Percent
Età	14	0	0
Rischio	14	0	0
Libertà	14	0	0
Tempistica	14	0	0
Sicurezza	14	0	0
Utilizzo sicurezza	14	0	0

Protezione salute	14	0	0
sistemi_smaltim	14	0	0
pratica_smaltim	14	0	0
furto_dati_person	14	0	0
Salvaguardia dati	14	0	0
Sesso	14	0	0

En el historial de los alumnos del instituto público, la falta de respuestas se concentra en las preguntas que requieren un poco más de conocimiento técnico, a las que los alumnos han decidido no responder. En los registros de los padres y maestros de los alumnos de la institución privada no había respuestas perdidas. Para ser precisos, sólo hubo una falta de respuesta en el apartado de los profesores.

**Tabla 6**

*Resumen de los valores que faltan en el registro de los padres de los alumnos del Instituto privado..*

	N	Missing	
		Count	Percent
Età	14	0	0
Rischio	14	0	0
Libertà	14	0	0
Tempistica	14	0	0
Sicurezza	14	0	0

utilizzo_sicurezza	14	0	0
protezione_salute	14	0	0
sistemi_smaltim	14	0	0
pratica_smaltim	14	0	0
furto_dati_person	14	0	0
salvaguardia_dati	14	0	0
Sesso	14	0	0

**Tabla 7**

*Resumen de los valores faltantes en el registro de los profesores de los alumnos del Instituto privado.*

	N	Missing	
		Count	Percent
Età	21	0	0
Rischio	21	0	0
Libertà	21	0	0
Tempistica	21	0	0
Sicurezza	21	0	0
utilizzo_sicurezza	20	1	4,8
protezione_salute	21	0	0

sistemi_smaltim	21	0	0
pratica_smaltim	21	0	0
furto_dati_person	21	0	0
salvaguardia_dati	21	0	0
Sesso	21	0	0

Por otra parte, en el historial de los alumnos de la institución privada, al igual que en el caso de la institución estatal, se concentraron mayores porcentajes de falta de respuesta en las preguntas que requerían más conocimientos técnicos.

**Tabla 8**

*Resumen. Faltan valores en el registro de los alumnos del Instituto privado.*

	N	Missing	
		Count	Percent
Virus	27	0	0
Cattivo_consiglio	25	2	7,4
Aggiornamento_PC	27	0	0
Antivirus_aggiornato	27	0	0
Antivirus_preinstallato	26	1	3,7
Password	27	0	0

Rischi_informatici	26	1	3,7
Pubblicazione_contenuti	27	0	0
Accesso_PC_pubblici	27	0	0
Cyberbullismo	27	0	0
Malware	23	4	14,8
Social_network	26	1	3,7
Social_network2	7	20	74,1
Icona_Mozilla	27	0	0
Ricorda_password	27	0	0
Phishing	25	2	7,4
Tre_R	27	0	0
Pericolosità_dispositivi	27	0	0
Ewaste	25	2	7,4
Gestione_rifiuti	27	0	0
Problema_salute_uno	27	0	0
Problema_salute_due	27	0	0

	N	Missing	
		Count	Percent

Lavoro_scrivania	27	0	0
Monitor_PC	27	0	0
Riduzione_rischi	27	0	0
Equilibrio_tra_mondi	27	0	0
Prenotazione_online	27	0	0
Dati_personali	27	0	0
Inserimento_file	27	0	0
Sfottò_virtuale	27	0	0
Pubblicazione_video	27	0	0
Invito	27	0	0
Email_banca	27	0	0
Navigazione_bimbi	27	0	0
Premio	27	0	0
Età	27	0	0
Ore_giorno_PC	20	7	25,9
Ore_giorno_tablet	20	7	25,9
Ore_giorno_cellulare	21	6	22,2
Rischio	25	2	7,4
Libertà	25	2	7,4
Navigazione_classe	24	3	11,1

Sesso	26	1	3,7
-------	----	---	-----

En cuanto al problema de la falta de respuesta, se ha tenido en cuenta que si falta un dato, no hay forma de saber cuál habría sido la respuesta del sujeto si lo hubiera dado. Por lo tanto, cada operación para llenar el vacío en el conjunto de datos implicará la inserción y el posterior análisis de un dato no observado realmente. Esto significa que cuanto mayor sea el porcentaje de datos faltantes estimados (en inglés, imputados) mayor será el grado de artificialidad del conjunto de datos. El hecho de que la estimación del valor se haya realizado mediante programas informáticos específicos y publicaciones que respaldan su fiabilidad, no cambia el hecho de que ese valor no se haya observado realmente. Dicho esto, "el procedimiento de compensación que se utiliza comúnmente para la falta de respuesta parcial es la imputación, que consiste en asignar un valor de reemplazo para los datos que faltan a fin de restablecer la integridad de la matriz de datos" (Olivieri, 2012). En la literatura se proponen varios métodos de imputación para predecir los valores de sustitución de la falta de respuesta parcial. En general, se pueden considerar tres clases de métodos:

1. Métodos deductivos, en los que el valor imputado se deduce de la información o los informes conocidos;
2. Métodos deterministas, en los que las imputaciones repetidas por unidad de las mismas características producen siempre los mismos valores imputados;
3. Métodos estocásticos, en los que imputaciones repetidas por unidad de las mismas características pueden producir diferentes valores imputados; se caracterizan por la presencia de un "componente aleatorio, que corresponde a un esquema probabilístico asociado al método particular de imputación elegido" (Signore et al., 2010).

El elegido, en esta área, es un método de imputación estocástica llamado asignación múltiple. Sólo para el seguimiento de los registros de los profesores del alumnado perteneciente al instituto privado, se decidió no considerar en el análisis la unidad estadística incompleta (porcentaje de falta de respuesta inferior al 5% del total de casos). La idea básica del "método de imputación múltiple" es generar más de un valor ( $m > 2$ ) a imputar por cada dato que falta,



de manera que las matrices completas de datos a analizar con métodos y programas informáticos estándar sean m” (Baccini, 2008).

### **5.1.2. Las etapas de la investigación**

El análisis consiste en que la administración de los cuestionarios siguió varias etapas en las que se sentaron las bases y los supuestos para una investigación lo más escrupulosa posible. Las fases:

Fase 1: el investigador se puso en contacto con el director de la escuela y le explicó los objetivos y métodos de la investigación que se llevaría a cabo en el Instituto en cuestión.

Fase 2: el director de la escuela sometió el asunto a la decisión del consejo de profesores. El colegio votó unánimemente a favor.

Fase 3: el investigador fue autorizado a entrar en las clases objeto de examen (administración de la tercera dirección, finanzas y marketing) en el plazo indicado por el director.

Fase 4: el investigador entró en el aula, sustituyendo a los profesores que decidieron salir del aula de forma autónoma. Se explicaron a los estudiantes los procedimientos para la administración del cuestionario, señalando que su colaboración habría sido totalmente anónima e individual, que se habría llevado a cabo con total autonomía, salvo aclaraciones o dificultades estrictamente de procedimiento. El tiempo disponible se cuantificó en 45 minutos.

Fase final: Según lo acordado con el director de la escuela, a la entrega del cuestionario completado, se pidió a los alumnos que se compararan con los demás alumnos en cada respuesta y en particular en las incorrectas. Los alumnos hicieron una serie de preguntas y pidieron más información sobre ciertos temas, demostrando su interés también con la rapidez con la que esperaban las respuestas. La discusión se llevó a cabo en una lluvia de ideas con los estudiantes que se turnaban para pedir la palabra.

### **5.1.3. La muestra**

Esta encuesta se llevó a cabo en relación con dos conjuntos de referencias:

- Uno compuesto por adolescentes, en su mayoría de 16 años, que asisten a las terceras clases de dos institutos (uno estatal y otro igual) de la escuela secundaria de tipo técnico con enfoque en administración, finanzas y mercadeo, del Municipio de Vittoria;
- El otro está formado por adultos, en su papel de profesores y padres de la muestra de alumnos examinados.

En el Municipio de Vittoria solo existen estos dos institutos técnico-comerciales. El Instituto Estatal tiene 4 terceras clases con la misma dirección, mientras que el Instituto privado<sup>7</sup>subvencionado solo una tercera clase. Para los estudiantes fue posible realizar una encuesta censal ya que fue posible llegar a todo el universo de referencia. La muestra de investigación está compuesta por 85 estudiantes que asisten a las clases de los dos institutos técnicos comerciales con especialización en administración, finanzas y marketing (estatales y privados). En cuanto a los adultos, sin embargo, no fue posible entrevistar a toda la muestra útil, es decir, a todos los padres y profesores de los alumnos examinados, debido a una actitud de desconfianza encontrada en ambas categorías. Solo una parte de los entrevistados manifestó su disposición a completar el cuestionario. Por tanto, la encuesta sobre adultos se trata como una encuesta por muestreo. El procedimiento utilizado para conformar la muestra es, por tanto, un muestreo accidental no probabilístico, dada la imposibilidad de realizar un muestreo probabilístico, debido al alto porcentaje de no encuestados. “Un muestreo accidental ocurre cuando el investigador elige a las primeras personas que cumplen con su encuesta, sin criterios definidos” (Bruni & Gobo, 2005). Incluso si el grado de precisión es menor, no son aplicables las técnicas de estadística inductiva, que se basa en procedimientos sistemáticos para verificar la importancia de una muestra de datos, relacionada con el tamaño y la representatividad de toda la población.

#### **5.1.4. Los criterios de evaluación**

La evaluación del componente ético relativo a la capacidad de comportarse adecuadamente en los entornos virtuales, con especial atención a las cuestiones de protección personal y respeto a los demás, se ha realizado sobre un máximo de 7 cuestiones éticas:

- Menos de 4: bajo nivel de conciencia de las implicaciones éticas de las tecnologías;

- De 4 a 5: nivel medio de conciencia;
- Más de 5: alto nivel de conciencia (Calvani, Fini & Ranieri, 2014).

Traducido en porcentajes:

- Menos de 5,71: bajo nivel de conciencia de las implicaciones éticas de las tecnologías;
- 5,71 a 7,14: nivel medio de conciencia;
- Más de 7,14: alto nivel de conciencia.;

Basándonos en esta evaluación, los criterios que aplicaremos serán:

- Número de preguntas correctas inferior a 14: bajo nivel de conciencia de las implicaciones éticas de las tecnologías.
- Número de preguntas correctas que van de 14 a 18: nivel medio de conciencia
- Mayor de 18 años: alto nivel de conciencia.

Las preguntas con una sola respuesta posible tuvieron una puntuación de 1 si la respuesta era correcta y cero si era incorrecta o faltaba. En las preguntas con más de una respuesta, la puntuación 1 se dio sólo cuando ambas respuestas fueron dadas correctamente. La falta o incorrección de una sola de las respuestas totalizó una puntuación igual a cero en cada caso. La elección de los términos y el contenido del cuestionario presuponen que los alumnos normalmente saben leer y escribir. Se supone que los alumnos también conocen el vocabulario especializado que encontrarán en el cuestionario: *file, virus, blog, posta elettronica, browser, sito di condivisione, icone, social network, scanner, chat, motore di ricerca, home page, allegato, grassetto, taglia/copia/incolla* (Calvani et al., 2014).

### **5.1.5. Instrumentos y validación del cuestionario**

El cuestionario propuesto a los alumnos se tomó de la batería de preguntas desarrolladas por Calvani (Calvani, Fini, & Ranieri, 2011). Las preguntas se administraron en algunas escuelas italianas y extranjeras y han experimentado pequeñas variaciones y mejoras resultantes de la práctica y la experiencia directa. La batería de aplicaciones fue validada primero mediante dos aplicaciones en escuelas italianas y luego traducida al inglés y al chino, para ser administrada

en China. (Li & Ranieri, 2010). A raíz de una aplicación en línea que permitió reunir datos de los alumnos de la escuela secundaria, se realizó un primer "análisis de elementos" significativo (Calvani et al., 2014). Posteriormente, se realizó otra encuesta en la que participaron más de mil estudiantes de secundaria. "La prueba confirmó un buen nivel de fiabilidad. De hecho, el valor del coeficiente alfa de Cronbach fue satisfactorio, tanto con la muestra china (0,77) como con la italiana (0,79) (Calvani et al., 2014). Los elementos reelaborados, reducidos y validados de ensayos anteriores se utilizaron para una encuesta posterior realizada en Italia en 2010. El número de participantes en la encuesta alcanzó los mil cincuenta y seis, estudiantes de 34 escuelas secundarias (Calvani, Fini, Ranieri, & Picci, 2012). Para la evaluación de los resultados también aplicaremos el umbral del 75% asumido como objetivo mínimo para ser considerados alumnos competentes en Seguridad Digital. Por otra parte, los cuestionarios dirigidos a los padres y profesores se han creado con el único propósito de identificar la posición adoptada por los adultos, con respecto a los riesgos de los cursos en Internet. El análisis de los resultados se utilizará para poner a prueba su opinión sobre la capacidad de sus hijos (en el primer caso) y de los estudiantes (en el segundo) para discriminar contra la información que se encuentra en línea. Las técnicas de encuesta utilizaron 3 cuestionarios modelados sobre los sujetos examinados. Más precisamente, se diseñó un cuestionario más largo y articulado para ser presentado a los estudiantes (el objetivo principal de esta investigación) y un cuestionario más corto y más inmediato para ser presentado a los padres y profesores. Los dos cuestionarios se componen de preguntas estructuradas (un conjunto cerrado de respuestas entre las que el entrevistado puede elegir) y de preguntas abiertas que dejan al entrevistado más libertad para responder. El primer cuestionario presenta dos áreas de la encuesta: una para explorar las características objetivas de la población objetivo y otra relativa a los conocimientos y el grado de aprendizaje de los entrevistados sobre los temas cubiertos por la encuesta. El segundo cuestionario se divide también en dos partes: una serie de preguntas destinadas a detectar características objetivas de la población y otra sección destinada a identificar opiniones sobre los temas de la encuesta. Por consiguiente, la información reunida es principalmente de carácter cualitativo y tiene por objeto obtener información sobre la situación actual y las expectativas de las principales variables estudiadas. La escala utilizada en la formulación de las respuestas estructuradas es la de Likert con 5 posiciones (Endler & Parker, 1990).

### 5.1.6. Procedimiento

La aplicación de la encuesta, en lo que respecta al alumnado, se llevó a cabo en el aula durante el horario escolar y dentro del tiempo previsto por el director y los profesores. La administración de los cuestionarios a los padres, por otra parte, se realizó durante las horas de tutoría. La administración de los cuestionarios a los profesores tuvo lugar en la sala de profesores. Antes de la administración de los cuestionarios, se explicó a los adultos entrevistados el propósito de la encuesta y la forma de rellenarla. A los alumnos sólo se les explicó cómo rellenar el cuestionario para no interferir en modo alguno en las respuestas. Para todos ellos el relleno se hizo de forma anónima y voluntaria. Una vez reunidos los cuestionarios, se preparó una rejilla de registro para dejar constancia de los datos que contenían.

En la práctica, se construyeron 6 rejillas de registro: 3 para el instituto estatal y 3 para el instituto privado, con el fin de diferenciar el análisis para los alumnos, los profesores y los padres. Cada rejilla muestra el tipo de campo, el ancho de los campos, las etiquetas de las variables, los códigos (La codificación de los datos es la fase en la que se asocia apropiadamente un código numérico a cada respuesta a cada pregunta) que se utilizarán en la compilación de las respuestas. Se ha proporcionado una codificación apropiada para las respuestas abiertas. Las parcelas se crearon con el programa informático SPSS Statistics, un completo sistema de análisis de datos para generar informes con tablas, gráficos de distribución y tendencias, estadísticas descriptivas y análisis estadísticos complejos. Los datos se introdujeron en las hojas de SPSS.17, y luego se procesaron en los siguientes pasos:

1. Revisión de los datos. La revisión, mediante un procedimiento automático, se refería a la identificación e imputación de valores faltantes o incoherentes de las variables examinadas, mediante los procedimientos que ofrece el programa informático utilizado;
2. Procesamiento estadístico. Las elaboraciones se llevaron a cabo mediante tablas y gráficos de frecuencias, en los que las distribuciones se representaron mediante el cálculo de las estadísticas descriptivas univariantes apropiadas. "Estos análisis se definen como análisis exploratorios de tipo simple e implican la síntesis de la información y su análisis por separado para cada variable detectada" (Fortini, Scanu, & Signore, 2000).

Los propósitos de este tipo de análisis son de tres tipos:

- Detección de errores en los datos, es decir: inconsistencias, omisiones y cualquier otra cosa que pueda ocurrir durante la entrada de datos;
- Identificar los modos de respuesta que son mal utilizados por los encuestados, y en este caso hacer las agrupaciones adecuadas, para evitar frecuencias demasiado bajas o incluso cero" (Bove, 2010).
- Obtener la primera información importante sobre el fenómeno, con referencia a las variables detectadas.

A continuación se realizaron análisis exploratorios multivariantes y se estimaron los parámetros de la población de referencia para la muestra de adultos.

3. Validación. Esta última fase permitió la evaluación de la información, más precisamente se estableció si podía considerarse adecuada, pertinente y significativa para los fines para los que se produjo.

Los objetivos del ejercicio de validación son dobles:

- Evaluar si la calidad de los datos es suficiente para la difusión de la información a los usuarios;
- Identificar las fuentes de error más relevantes". (Fortini, Scanu, & Signore, 2000).

### **5.1.7. El cuestionario**

Nuestra investigación se refirió al concepto de Seguridad de la Información proporcionado por Antonio Calvani y otros, (2011). Al igual que estos últimos, hemos considerado la subdivisión del tema en 4 áreas o categorías. Basándonos en estos estudios, las 4 áreas se definen de la siguiente manera:

1. La protección de la salud que incluye:

- Concienciación por parte de los estudiantes de que existen riesgos para la salud relacionados con el uso de la tecnología digital (por ejemplo, riesgo de adicción, problemas ergonómicos);
- Prevención de problemas de salud (físicos y psicológicos);

- Uso razonable de las tecnologías de la información y la comunicación.

## 2. La protección de los datos personales que incluye:

- Riesgos relacionados con el robo de credenciales (nombre de usuario y contraseña);
- El peligro de revelar información personal en línea;
- La necesidad de tener múltiples contraseñas para acceder a sus dispositivos y servicios digitales, y la necesidad de cambiarlas periódicamente;
- La capacidad de identificar sitios web o correos electrónicos que pueden ser fraudulentos, así como correos electrónicos de phishing;
- El conocimiento de herramientas para encriptar correos electrónicos o archivos;
- El conocimiento y uso de procedimientos para aplicar filtros para el correo electrónico (spam).

## 3. Protección del equipo informático, que abarca:

- La necesidad de tomar precauciones específicas para proteger los dispositivos de la computadora con el antivirus, la contraseña y el cortafuegos;
- La oportunidad de comprobar frecuentemente la configuración y los sistemas de seguridad de sus dispositivos o aplicaciones.

## 4. La protección del medio ambiente, que incluye:

- Conocimiento de las principales medidas de ahorro de energía;
- Conciencia de que el impacto de la tecnología en el medio ambiente puede tener un resultado positivo y negativo en relación con el comportamiento adoptado.

Todos los artículos se basan en problemas reales que el estudiante enfrenta frecuentemente mientras navega por la red. También se han tenido en cuenta las contribuciones de Jenkins y del New Media Literacy Team (Calvani, Fini y Ranieri, 2010), que exploran el área ética, de Limburg (1989), de Marturano (Marturano, 2010) que abordan las cuestiones de la privacidad, la identidad, la credibilidad, la participación, la propiedad y el derecho de autor. Las preguntas del cuestionario, que se propuso a los alumnos, se referirán también a los conceptos

de protección del medio ambiente, respeto a los demás y conciencia de los posibles riesgos. El cuestionario está estructurado de la siguiente manera:

- Preguntas cerradas de opción múltiple; con la posibilidad de añadir un comentario al final del cuestionario;
- Pruebas localizadas que evaluarán la competencia de seguridad en línea en la situación, la capacidad del alumno para participar de forma constructiva y consciente en la sociedad social y del conocimiento y la sociedad de la información. Se tendrá en cuenta un comportamiento consciente, seguro y apropiado en la interacción con los demás.

Los cuestionarios, en el único sentido de Seguridad en línea, de nuestra relevancia, han sido sometidos a una nueva evaluación por un equipo de profesores: un profesor de matemáticas, el Profesor N., con más de cuarenta años de experiencia en la enseñanza de las matemáticas y la informática, el pedagogo, el Profesor C., y el Profesor P., profesor de apoyo, experto en informática. Las pruebas también permitirán al estudiante autoevaluarse y verificar la corrección de su comportamiento en línea. Los temas se profundizarán en el aula, mediante un diálogo abierto con el profesor/investigador, que seguirá el cumplimiento de los cuestionarios. Por otra parte, los cuestionarios dirigidos a los padres y maestros se utilizarán para poner a prueba y vigilar su confianza en la capacidad de los niños y estudiantes para discriminar la información en línea. A modo de conclusión y teniendo en cuenta los beneficios de la utilización de la tecnología en la educación, se pretende investigar el nivel de competencia, en el reconocimiento y la neutralización de las amenazas en línea, que poseen los alumnos que asisten al tercer curso de la escuela secundaria de los dos institutos objeto de estudio. Esta investigación pretende:

- profundizar en el concepto de seguridad digital que poseen los estudiantes en las tres perspectivas de observación del fenómeno (estudiantes, profesores y padres);
- analizar y comparar los datos de las dos Escuelas (estatales y privados);
- hacen una propuesta para una mayor seguridad en la escuela de la información.

El campo de investigación examinado se circunscribe a dos institutos de segundo grado: una pública y otra privada, y ambas localizadas en la provincia de Ragusa. En los dos institutos se



proponen distintas estrategias metodológicas de investigación, destinadas a descubrir el nivel de competencia en materia de seguridad informática que poseen los alumnos del tercer curso. La mayoría del alumnado de este curso tiene ya 16 años, edad en la que en Italia acaba la escolaridad obligatoria y, por tanto, en la que ya se deberían haber adquirido ciertas habilidades informáticas en una ciudadanía activa y consciente.



## **CAPÍTULO VI**

### **Exposición y comentario de resultados**

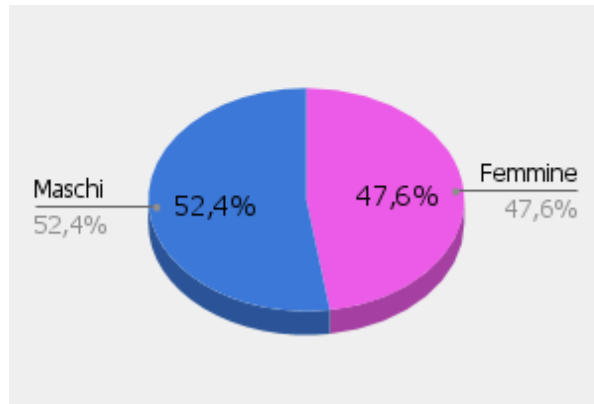
#### **6.1. Comparación de resultados según tipología de centro**

##### **6.1.1. Análisis de los resultados del centro escolar público**

La muestra de docentes del instituto técnico-comercial estatal está conformada por 21 sujetos con edades comprendidas entre los 40 y los 64 años, lo que presenta una buena distribución uniforme por sexo y tipo de docencia (ver gráfico 1 y 2).

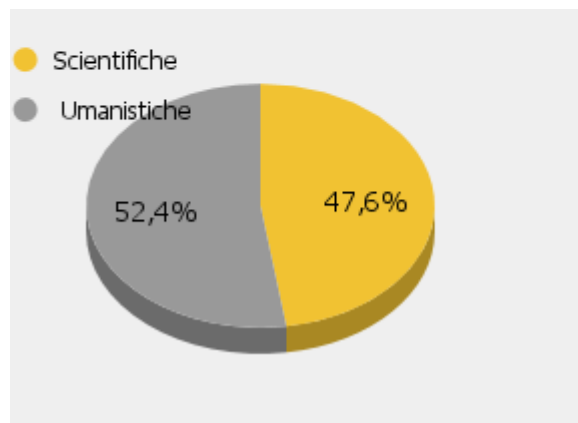
### Gráfico 1

*Distribución por sexo de los profesores del Instituto Estatal X*



### Gráfico 2

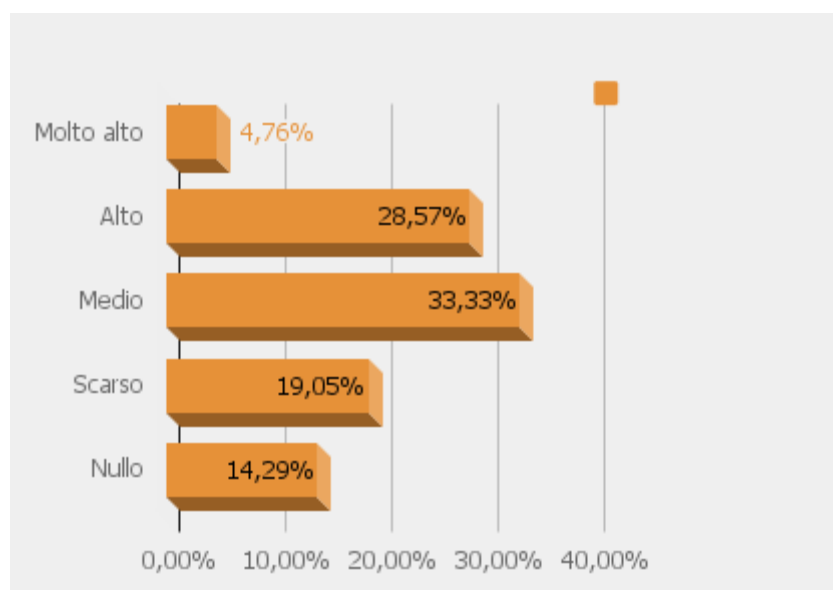
*Distribución por tipo de enseñanza de los profesores entrevistados*



Ante la siguiente pregunta: “¿Qué nivel de riesgo perciben los niños cuando navegan por la red?”, la mayoría del profesorado de la escuela pública considera que ese riesgo es de nivel medio-alto.

### Gráfico 3

El riesgo percibido por los estudiantes en la opinión de los profesores



Crean que los estudiantes perciben claramente un cierto grado de riesgo cuando navegan por la red, y que esta percepción es de valores medio-altos. Al mismo tiempo, los propios profesores están convencidos de que dan a sus alumnos demasiada libertad para usar los teléfonos móviles en el aula.

### Tabla 9

*Distribución de frecuencias de los modos de respuesta a la pregunta sobre la libertad en el aula de usar el teléfono móvil*

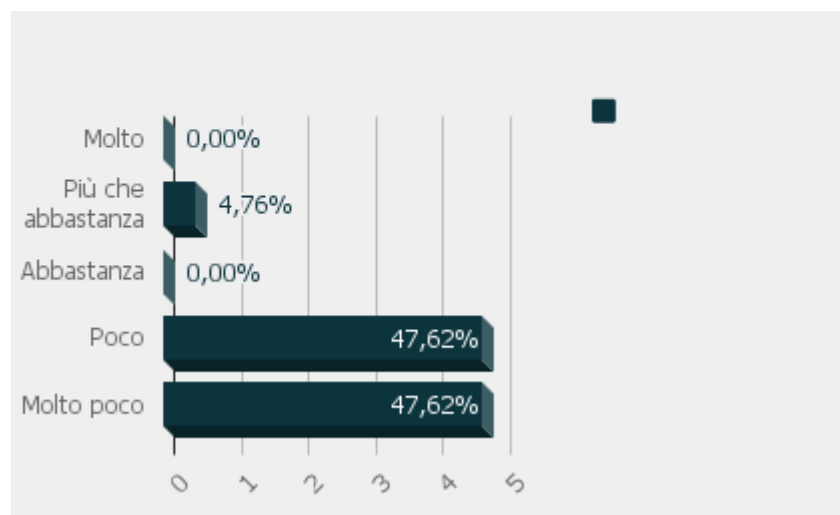
	Frequency	Percent	Valid Percent	Cumulative Percent
Alta	4	19	19	19
Media	8	38,1	38,1	57,1
Scarsa	4	19	19	76,2
Nulla	5	23,8	23,8	100

Total	21	100	100	
-------	----	-----	-----	--

Sin embargo, por otra parte, son conscientes de que la navegación en las aulas con fines educativos es pequeña e insuficiente para explotar la utilidad potencial de la red con fines de estudio y enseñanza (más del 70% de los profesores, de hecho, contestan que el tiempo dedicado es poco o muy poco). En cuanto a los sistemas de seguridad, poco más del 57% de los maestros están seguros de que los niños saben poco o nada sobre el tema. Este porcentaje aumenta al 76% cuando se trata de la aplicación de sistemas de seguridad. Las cifras son preocupantes cuando se trata de proteger la salud del uso excesivo del PC, más del 95% de los profesores están convencidos de que los alumnos no saben cómo protegerse.

#### Gráfico 4

*La opinión de los profesores sobre el comportamiento de los estudiantes para proteger su salud del uso excesivo del PC*

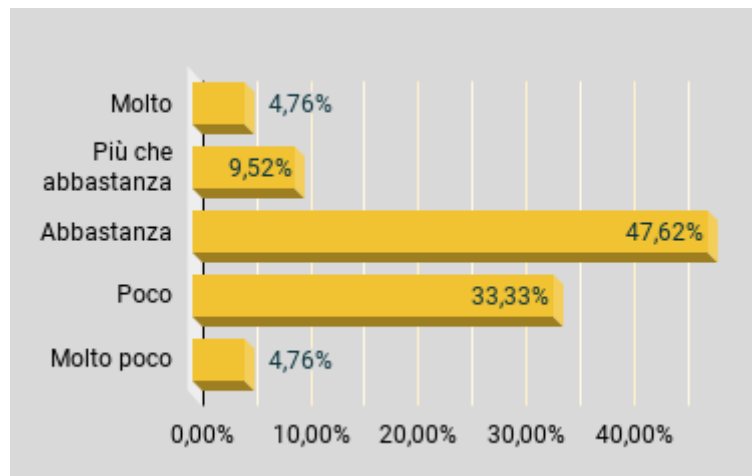


Hay, pues, un 90% que cree en la ignorancia de los jóvenes sobre los sistemas de eliminación de los dispositivos informáticos y más del 95% de los encuestados muestran desconfianza en su capacidad para adoptarlos. Los profesores, sin embargo, confían en que sus hijos sepan que

los datos personales en Internet pueden ser robados. Más del 60% del profesorado considera que serán bastante conscientes a largo plazo, pero también creen que no hacen nada para protegerse del robo (ver Gráfico 5 y [Tabla 8](#)).

### Gráfico 5

*Opinión de los profesores sobre la conciencia de los estudiantes del riesgo de robo de cursos en Internet con respecto a los datos personales.*

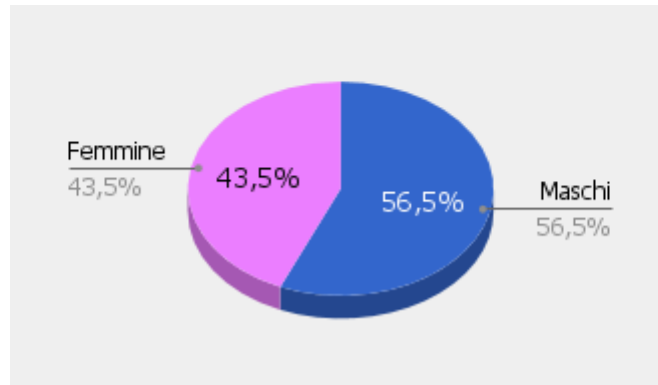


### Análisis de los cuestionarios de los alumnos del instituto estatal

La parte más interesante de este estudio es el análisis de los datos obtenidos a partir de los cuestionarios cumplimentados por el alumnado. La encuesta se refiere a los conocimientos de los estudiantes en relación con el uso de los dispositivos informáticos y los factores de riesgo. También se refiere a las opiniones y opiniones expresadas por los estudiantes en relación con los peligros de la navegación por Internet. La muestra de alumnos está compuesta por 85 sujetos de entre 15 y 19 años de edad (edad media de 16 años y medio), con una ligera preponderancia de los varones sobre las mujeres. El número real de estudiantes que asisten a las 4 clases del instituto estudiado llega a 100, pero la encuesta, debido al absentismo, sólo alcanzó 85. El 56,5% de ellos eran hombres. (ver gráfico 6).

## Gráfico 6

*Distribución por sexo de los alumnos del instituto estatal*



Los datos críticos provienen del número de horas que los estudiantes afirmaron pasar frente a los dispositivos electrónicos. Particularmente frente a los teléfonos móviles, el promedio es cercano a las 7 horas diarias con picos de hasta 20 horas diarias, mientras que para la tableta hay un 87% de estudiantes que no hacen uso pleno de ellas. El teléfono móvil es utilizado por todos durante al menos una hora al día, pero hay un alarmante 20% que lo utiliza durante más de 10 horas al día y sólo el 9,4% dice que lo utiliza de 0 a 2 horas.

## Tabla 10

*Número de horas/día pasadas frente a la PC, la tableta y el teléfono móvil*

	N	Minimum	Maximum	Mean	Std. Deviation
Ore_giorno_PC	85	0	10	1,37	1,708
Ore_giorno_tablet	85	0	2	0,17	0,452
Ore_giorno_cellulare	85	1	20	6,8	4,818

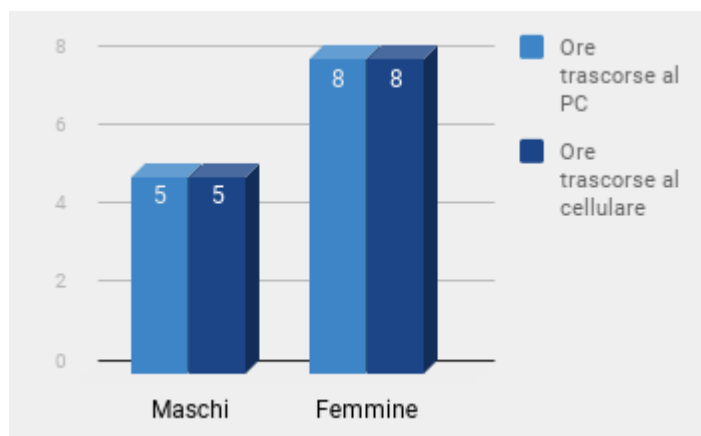


Valid N (listwise)	85				
--------------------	----	--	--	--	--

Haciendo una distinción por sexo se puede decir que las mujeres utilizan el teléfono móvil durante más tiempo que los hombres (más de 5 horas para los hombres frente a más de 8 horas para las mujeres).

### Gráfico 7

*Distribución por sexo del número de horas al día que se pasan frente a un dispositivo informático*



La primera serie de preguntas del cuestionario que se da a los alumnos se refiere a la protección del equipo informático. Los alumnos parecen estar bastante preparados en este tema, tanto porque hay bajos niveles de falta de respuesta como porque las respuestas dadas son generalmente correctas. Los resultados obtenidos para este conjunto de preguntas son:

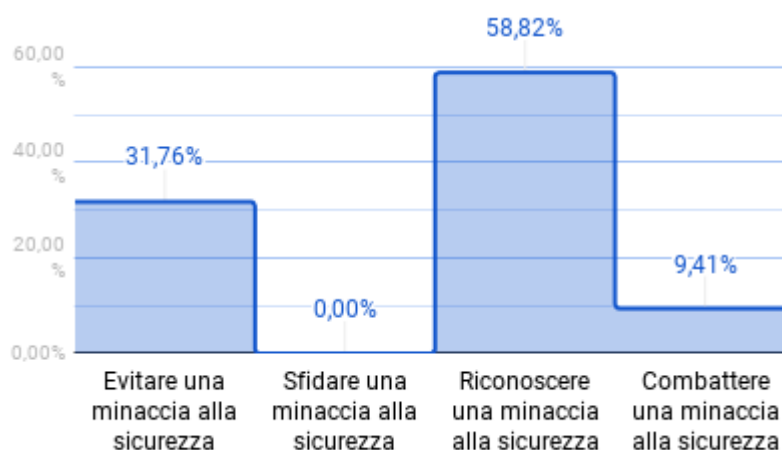
- Más del 95% sabe para qué sirve un programa antivirus;
- Más del 80% conoce la definición correcta de virus;
- Casi el 85% sabe que abrir los archivos adjuntos de un correo electrónico que le interesan no es recomendable para la protección de su PC;

- El 65% es consciente de que es aconsejable mantener su sistema operativo actualizado con la última versión disponible;
- Más del 85% sabe que mantener su antivirus actualizado no significa que su PC no pueda ser infectado de todos modos;
- El 86% sabe que el software antivirus preinstalado al momento de la compra no es suficiente para proteger su computadora;
- Casi todo el mundo sabe la mejor manera de crear contraseñas.

La segunda secuencia de preguntas se refiere a la protección de los datos personales. Se les preguntó a los niños cuál era el primer paso para protegerse de los riesgos cibernéticos. Casi el 60% de los encuestados respondieron correctamente (es decir, reconocen una amenaza a la seguridad con antelación). Afortunadamente, nadie respondió "desafiando una amenaza a la seguridad". (ver gráfico 8)

### Gráfico 8

El primer paso para protegerse de los riesgos cibernéticos



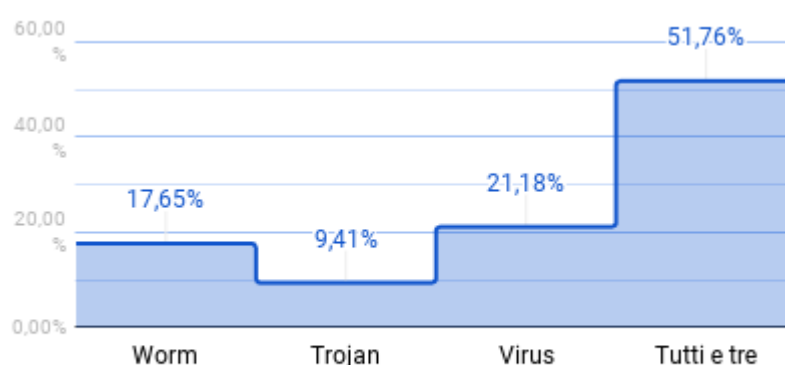
Además, casi el 90% de los alumnos de la institución estatal son conscientes de que una vez que un contenido se publica en Internet, siempre hay un rastro del mismo y que no es seguro acceder a sus datos personales desde un ordenador público.

Casi todos, es decir, el 98,8%, conocen los canales de ataque del ciberacoso.

Los jóvenes están un poco menos preparados en lo que respecta a los programas informáticos maliciosos (poco más de la mitad reconoce la definición correcta, pero el resto parece muy confuso).

## Gráfico 9

### Definición de malware



La pregunta sobre el mejor uso de las redes sociales tenía una doble respuesta. La mayoría de los chicos respondieron correctamente a ambas respuestas.(ver cuadro 9)

## Tabla 11


### La mejor manera de usar las redes sociales

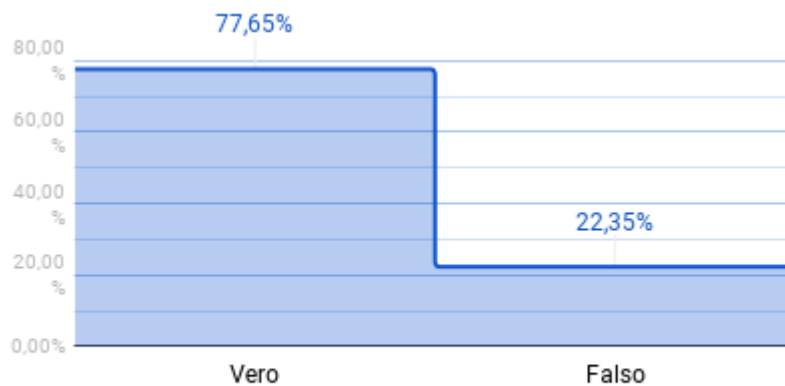
Modalità di risposta	1^ risp		2^ risp	
	N	%	N	%
Contare su impostazioni di sicurezza predefinite.	6	7,10%	21	24,70%
Impostare la privacy e le	60	70,60%	9	10,60%

impostazioni di sicurezza in base al proprio livello di comfort personale per la condivisione delle informazioni.				
Evitare la condivisione di foto compromettenti e informazioni personali.	19	22,40%	55	64,70%

A la siguiente pregunta, referente al icono que aparece en Mozilla Firefox cuando se navega de incógnito, 4 de 5 han respondido correctamente reconociendo el símbolo.

### Gráfico 10

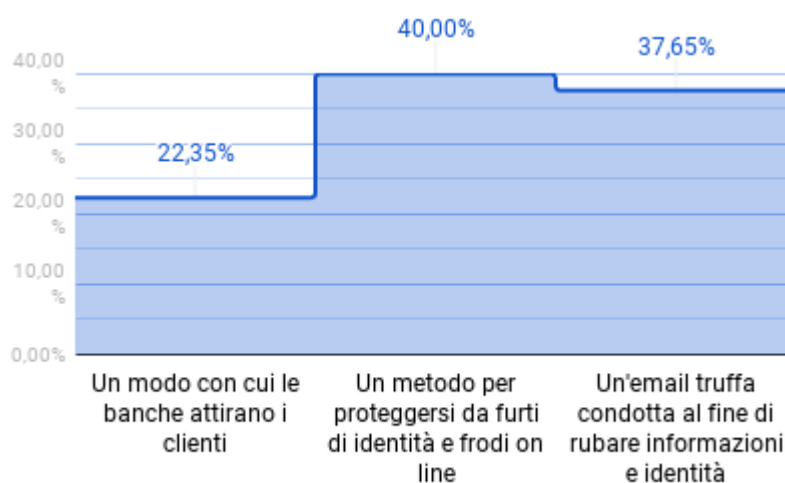
¿El icono de Mozilla indica que estoy navegando de incógnito? 



Sólo el 37, 65% de los encuestados conocen el término "phishing", por lo que sabrían cómo proteger sus datos, mientras que el 60% restante no conoce el término (esta definición es una de las preguntas más técnicas en las que se produjo el mayor porcentaje de falta de respuesta).

## Gráfico 11

### Definición de phishing



Casi todo el mundo sabe también que, si se accede al correo electrónico desde un ordenador público, al cerrar el navegador no es aconsejable utilizar la opción de recordar la contraseña. En lo que respecta a la definición de las tres R, el porcentaje de respuestas correctas ha alcanzado casi el 50%, la incertidumbre en la respuesta ha llevado a un alto valor de respuestas perdidas. Esta pregunta es la primera de una serie sobre "Protección del Medio Ambiente".

## Tabla 12

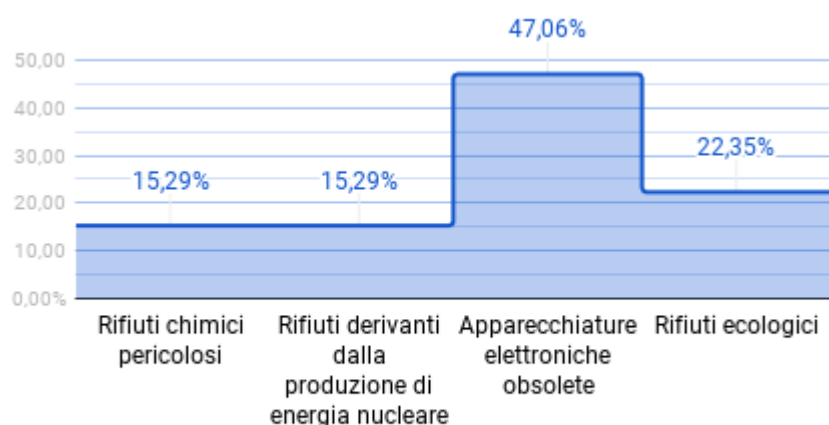
### La definición de las tres R de residuos

		Frequency	Percent	Valid Percent
Valid	Ridurre-rispettare-riciclare	32	37,6	37,6
	Ridurre-riutilizzare-riciclare	42	49,4	49,4
	Ridurre-riconsiderare-rispettare	11	12,9	12,9
	Total	85	100	100

La tasa de respuesta correcta se reduce aún más (hasta el 33%) cuando se plantea la cuestión de la peligrosidad de los dispositivos electrónicos. El colectivo se divide en tres partes casi perfectas, mientras que se divide en dos partes en lo que se refiere al término residuos electrónicos (y en esta pregunta se advierte la alta tasa sin respuesta). La pregunta "¿Cuál es la opción menos útil para la gestión de residuos?" tampoco alcanza el 50% de las respuestas correctas. La opción correcta de "eliminación" es un poco más del 43%.

## Gráfico 12

*Definición de e-waste*



## Tabla 13

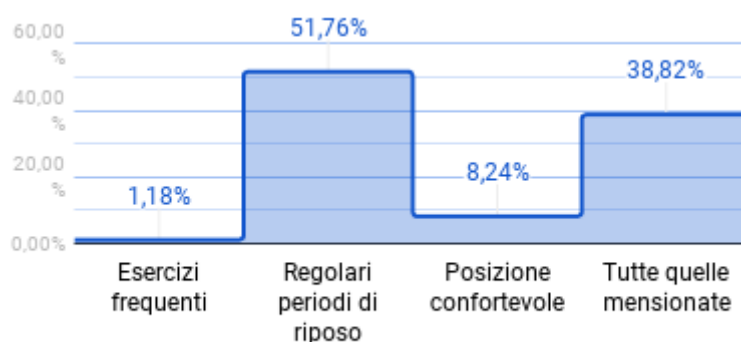
*La opción menos útil para la gestión de los desechos*

		Frequency	Percent	Valid Percent
Valid	Riuso	29	34,1	34,1
	Recupero	19	22,4	22,4
	Smaltimento	37	43,5	43,5
	Total	85	100	100

La penúltima serie de preguntas se refiere a la protección de la salud. En este tema los estudiantes tuvieron un mayor porcentaje de respuestas correctas que en el tema anterior, excepto en la primera pregunta relativa a los problemas de salud causados por escribir durante horas en el teclado sólo el 37,6% respondió correctamente "Lesiones por esfuerzo repetitivo". La mayoría se detuvo con problemas de espalda. Casi todo el mundo (alrededor del 90%), por otro lado, sabe que el parpadeo de la pantalla causa fatiga ocular y el 100% sabe cómo sentarse en un escritorio para evitar problemas de espalda. Cuando se preguntó sobre la disposición del monitor en relación con el nivel de los ojos, el 60% o más se equivocaron. En cuanto a las otras dos preguntas, por otra parte, al tener "todos los mencionados" como respuesta correcta, no se realizó el examen de las respuestas incorrectas porque no eran significativas para el análisis (véanse los gráficos 14 y 15 infra). Con respecto a la pregunta "¿cómo mantener el equilibrio entre el mundo virtual y el mundo real?" se especificó que el término virtual no se refiere a algo que no es real o no es real, sino simplemente a identificar y diferenciar los canales de comunicación de la red y el comportamiento fuera de línea.

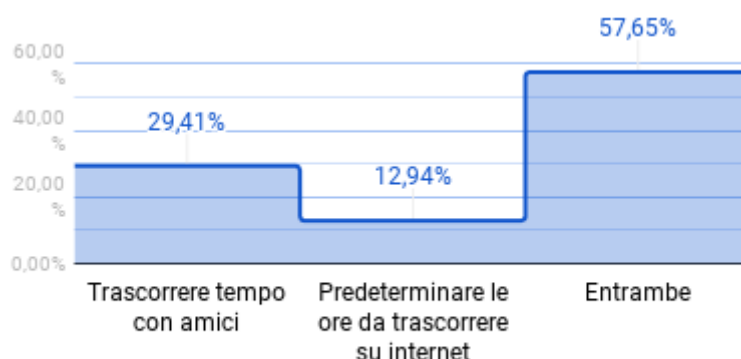
### Gráfico 13

*Cómo reducir los riesgos para la salud causados por el uso prolongado del ordenador*



## Gráfico 14

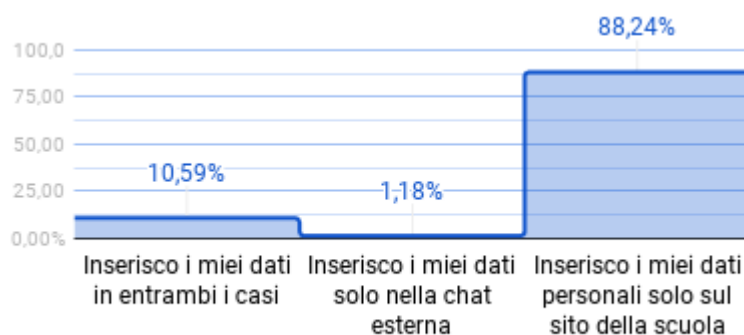
*Cómo mantener un equilibrio entre el mundo virtual y el real*



El último conjunto de preguntas se refiere al estudio de algunos casos concretos que deben ser examinados. La primera se refiere a la posibilidad de pagar una entrada para el concierto en línea. Un poco más de la mayoría de los alumnos (57,6%) piensa que es posible pagar con tarjeta de crédito después de verificar que el sitio adopta un cierto tipo de protección. A la siguiente pregunta Sobre el sitio en el que introducir los datos personales con cierto grado de seguridad, si en el sitio web de la escuela o en un chat externo, los alumnos no tienen ninguna duda y casi el 90% de ellos responden correctamente (véase el gráfico 15), lo que demuestra, por lo tanto, que se comportan con precaución en este caso.

## Gráfico 15

*¿En qué sitio es más seguro introducir sus datos personales? ¿En el sitio web institucional de la escuela o en un chat externo o ambos?*





Y aún así se respondió casi unánimemente que era un comportamiento completamente inaceptable para burlarse de los defectos de alguien en su blog.

**Tabla 14**

*Burlarse de los defectos de alguien en su blog*

		<i>Frequency</i>	<i>Percent</i>	<i>Valid Percent</i>
Valid	Non approvi l'atteggiamento, ma parteciperesti allo scherzo	2	2,4	2,4
	E' un comportamento del tutto inaccettabile	83	97,6	97,6
	Total	85	100	100

La pregunta que sigue a continuación "¿Qué problemas plantea la inclusión de audio, vídeo y fotografías personales en la red? La respuesta requiere más conocimientos técnicos e incluso en este caso, ha habido un elevado número de no respuestas y un porcentaje de respuestas correctas inferior a la media. Con demasiada frecuencia, los jóvenes muestran indudables aptitudes para el uso, pero éstas no están respaldadas por un conocimiento adecuado de los instrumentos, los contextos, los idiomas y los protocolos de comunicación, por lo que no se convierten en una verdadera competencia y conciencia de los medios, tanto en lo que respecta a las oportunidades que ofrecen como a los riesgos asociados a su uso. En este sentido, los organismos educativos, en primer lugar las escuelas, deben pensar en proyectos educativos que no sólo tengan por objeto promover las aptitudes de los usuarios, como se observa a menudo en el panorama educativo actual, porque al hacerlo sólo proporcionan una parte limitada y limitante de los instrumentos necesarios para el desarrollo de un usuario capaz de explotar eficazmente el potencial de las herramientas informáticas. El desconocimiento de los

mecanismos de funcionamiento de las redes, a todos los niveles, expone a riesgos que difícilmente pueden ser estimados.

**Tabla 15**

*¿Qué problemas plantea la inclusión de audio, vídeo y fotografías personales en los sitios web?*

		Frequency	Percent	Valid Percent
Valid	Rispetto delle clausole d'uso stabilite dagli autori	40	47,1	47,1
	Titolazione e commento dei materiali da parte di chi accede al sito	9	10,6	10,6
	Riproduzione dei materiali digitali scaricati	15	17,6	17,6
	Inserimento/scaricamento di materiali nel sito	21	24,7	24,7
	Total	85	100	100

**Tabla 16**

*Invitación por correo electrónico a una fiesta a una dirección desconocida*

		Frequency	Percent	Valid Percent
Valid	Non accetti l'invito perché non conosci le persone	52	61,2	61,2

	Accetti l'invito ma dopo aver chiesto più informazioni sul tema della festa	21	24,7	24,7
	Chiedi il parere di qualche amico	12	14,1	14,1
	Total	85	100	100

Por otra parte, una gran mayoría, un porcentaje del 90%, son conscientes de que la publicación de un vídeo requiere el consentimiento de todos los que aparecen en él. Las siguientes preguntas, por otra parte, tienen porcentajes más bajos de respuestas correctas, pero superiores al 60% (véanse los cuadros 14 y 15).

**Tabla 17**

*¿Qué consejo le daría a su abuelo que recibe un correo electrónico con el logo del Banco donde depositó sus ahorros, que contiene la solicitud de códigos de acceso y contraseñas?*

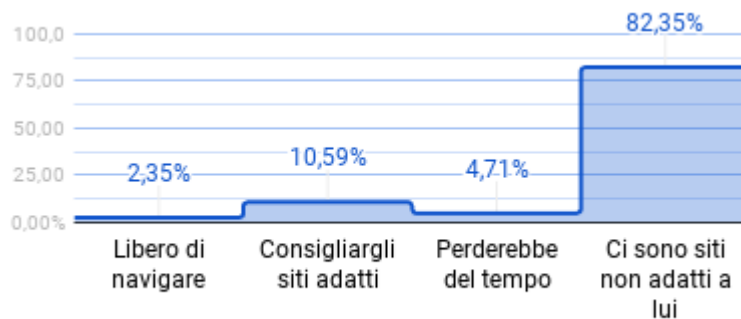
		Frequency	Percent	Valid Percent
Valid	Di fornire i dati richiesti se nel messaggio c'è il nome del direttore/mittente	12	14,1	14,1
	Di fornire i dati se nel messaggio c'è il logo della banca	8	9,4	9,4
	Di non rispondere aggiungere allo spam e se del caso avvisare la polizia postale	56	65,9	65,9

Di fornire i dati se conoscono l'indirizzo e-mail sono dipendenti della banca	9	10,6	10,6
Total	85	100	100

Más del 80% tiene bastante claro que para un niño de 8 años de edad, navegar libremente por Internet puede ser una elección imprudente e igualmente imprudente puede ser proporcionar datos personales en un sitio que llama la atención con la oferta de premios. (ver Gráfico 17 y 18).

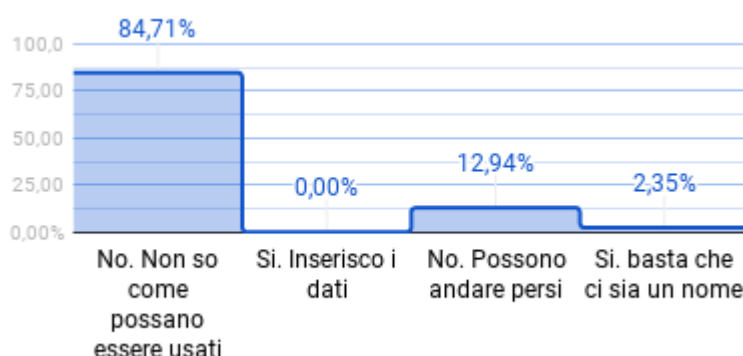
### Gráfico 16

*Navigar gratis por Internet para un niño de 8 años*



## Gráfico 17

*Proporcionar información personal en un sitio que ofrece recompensas*



A fin de determinar si existía algún tipo de relación entre la edad y el tipo de respuesta dada (correcta o incorrecta) a una pregunta ligeramente más técnica, se hicieron correlaciones bivariadas entre la variable de la edad y la pregunta de interés. Entre todas las realizadas, no se encontraron correlaciones significativas con la prueba de las dos colas de la Plaza Chi de Pearson. Al final del cuestionario también se hicieron preguntas a los estudiantes para conocer sus opiniones y puntos de vista. El primero de ellos se refería al riesgo percibido al navegar por la red. Para más del 50% el riesgo percibido es medio-alto. Más del 80% da un peso medio-bajo a la libertad de usar teléfonos móviles en clase y de navegar por Internet con fines educativos.

### 6.1.2. Análisis de los resultados de la escuela privada / concertada

Los profesores y los padres de la institución paritaria

También en este caso el análisis parte de la opinión de los profesores y los padres. La muestra de profesores consiste en 21 sujetos de entre 28 y 75 años de edad. El abanico, en el caso de la escuela privada, se amplía, enriqueciéndose con profesores más jóvenes y aún mayores, con una edad media de 48 años, mientras que, desde el punto de vista del sexo, sigue habiendo una buena distribución igualitaria entre hombres y mujeres, pero con un desequilibrio a favor de las mujeres hacia las humanidades.

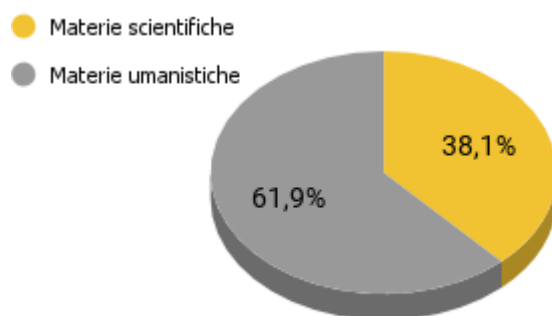
**Tabla 18**

*Distribución por sexo de los profesores del instituto técnico-comercial del igual número de profesores*

		Frequency	Percent	Valid Percent
Valid	Maschi	11	52,4	52,4
	Femmine	10	47,6	47,6
	Total	21	100	100

**Gráfico 18**

*Distribución por tipo de enseñanza (igual "G.Verga")*



En opinión de los profesores de la escuela privada, el riesgo percibido por los estudiantes mientras navegan por la red es medio-alto. De hecho, el 67% de los encuestados declaró un valor medio o muy alto. Según los profesores de la institución paritaria, la libertad de utilizar teléfonos móviles en el aula es baja (véase el cuadro 17). De hecho, solo el 5% respondió que es alto (correspondiente a un solo profesor). Los profesores también consideran que el tiempo dedicado a navegar por Internet con fines didácticos es reducido (en el 90% de los casos).

**Tabla 19**

*La opinión de los profesores sobre la libertad de los alumnos de usar teléfonos móviles en el aula*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nulla	2	9,5	9,5	9,5
	Scarsa	6	28,6	28,6	38,1
	Media	12	57,1	57,1	95,2
	Alta	1	4,8	4,8	100
	Total	21	100	100	

Los profesores del instituto privado, por otro lado, creen (casi el 86%) que sus hijos están bien informados sobre los programas de seguridad informática, aunque el 75% está dispuesto a argumentar que no los utilizan o, en todo caso, los utilizan de forma muy limitada.

**Tabla 20**

*La opinión de los profesores sobre lo bien informados que están los jóvenes sobre los programas de seguridad*

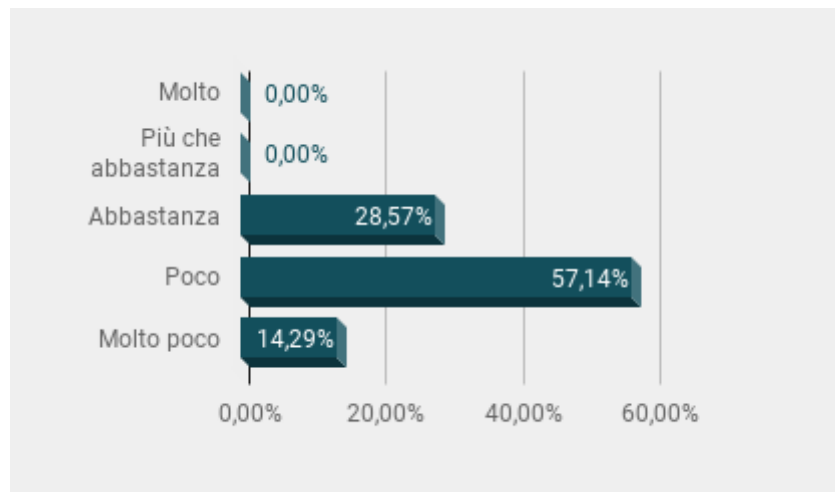
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Più che abbastanza	1	4,8	4,8	4,8
	Abbastanza	17	81	81	85,7

	Poco	1	4,8	4,8	90,5
	Molto poco	2	9,5	9,5	100
	Total	21	100	100	

Una vez más, cuando se trata de proteger la salud del uso excesivo del PC, más del 70% de los profesores están convencidos de que los alumnos no saben o no quieren protegerse.

### Gráfico 19

*La opinión de los profesores sobre los dispositivos adoptados por los estudiantes para proteger su salud del uso excesivo de la PC*



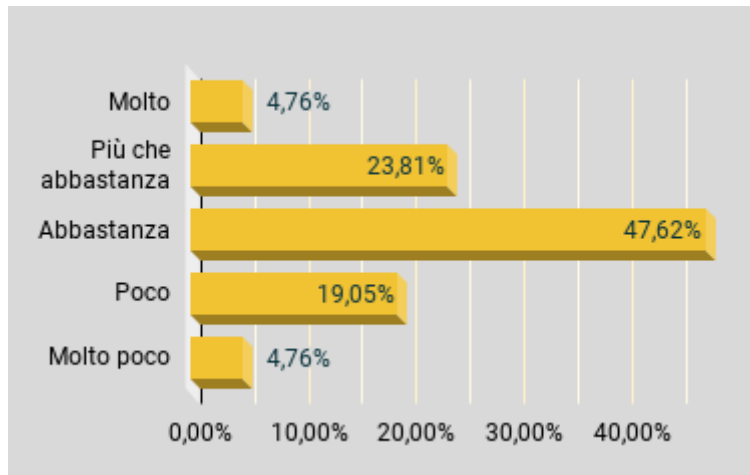
Además, el 76,2% de los encuestados están seguros de que los alumnos desconocen los sistemas de eliminación de dispositivos informáticos. Todos los profesores también creen que son incapaces de adoptarlos. Sin embargo, están seguros de que sus alumnos son conscientes de la posibilidad de que sus datos personales difundidos en Internet puedan ser robados (véase



el gráfico 20). Sin embargo, más del 60% cree que los estudiantes son incapaces o no están dispuestos a activar cortafuegos de protección.

### Gráfico 20

*La opinión de los profesores sobre el conocimiento de los estudiantes de la posibilidad de robo de datos personales en Internet*



### Tabla 21

*La distribución sobre la práctica de conductas dirigidas a salvaguardar los datos personales responde a los profesores*

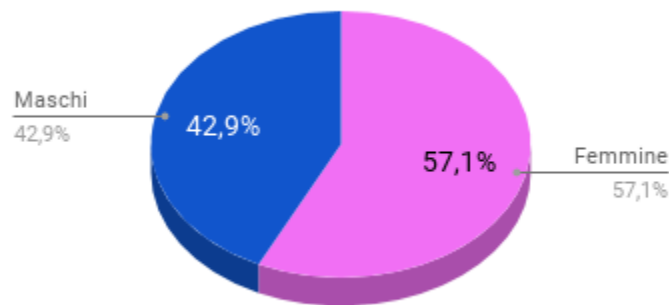
	Frequency	Percent	Valid Percent	Cumulative Percent
Molto poco	4	19	19	19
Poco	12	57,1	57,1	76,2
Abbastanza	4	19	19	95,2
Più che abbastanza	1	4,8	4,8	100

Total	21	100	100	
-------	----	-----	-----	--

La muestra parental del instituto técnico-comercial privado está más equilibrada entre hombres y mujeres que la del instituto público. (ver Gráfico 21).

### Gráfico 21

*Distribución por sexo de los padres de la institución paritaria*



Una vez más, los padres (alrededor del 86%) de la muestra del instituto provado creen que sus hijos perciben que sus hijos corren un riesgo medio al navegar por Internet. También saben que en el aula sus hijos no tienen ninguna posibilidad, o muy limitada, de usar teléfonos móviles.

### Tabla 22

*Posibilidad de utilizar los teléfonos móviles en el aula según la opinión de los padres de la institución paritaria*

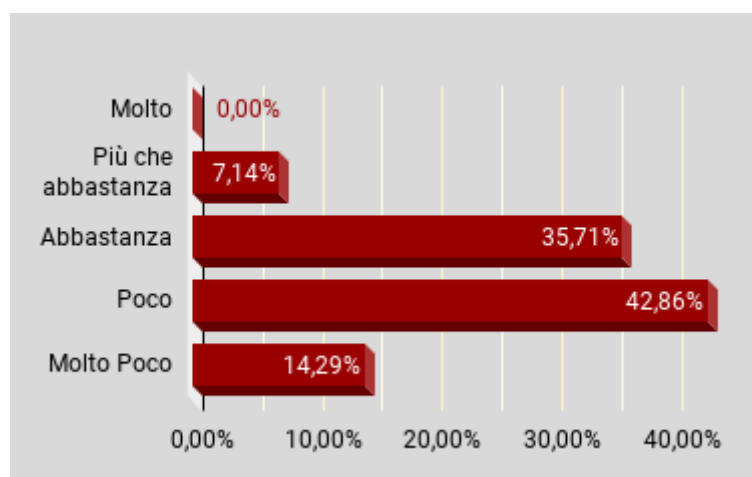
		Frequency	Percent	Valid Percent	umulative Percent
Valid	Nulla	2	14,3	14,3	14,3

	Scarsa	6	42,9	42,9	57,1
	Media	6	42,9	42,9	100
	Total	14	100	100	

Al igual que los profesores, creen (64%) que el tiempo que se pasa en el aula con fines de enseñanza es escaso. Al igual que los profesores, los padres están convencidos de que sus hijos están suficientemente informados sobre la existencia de los sistemas de seguridad. De hecho, casi el 80% da una respuesta que va de suficiente a mucho, mientras que en lo que respecta al uso de estos sistemas por parte de los estudiantes, el 57% está convencido de que se utilizan poco o nada. Es llamativo que las respuestas del profesorado van en la misma tendencia que la de los padres el instituto privado, cuyo 57% (que responde poco y muy poco) cree que sus hijos no son capaces de proteger su salud del uso excesivo del PC.

## Gráfico 22

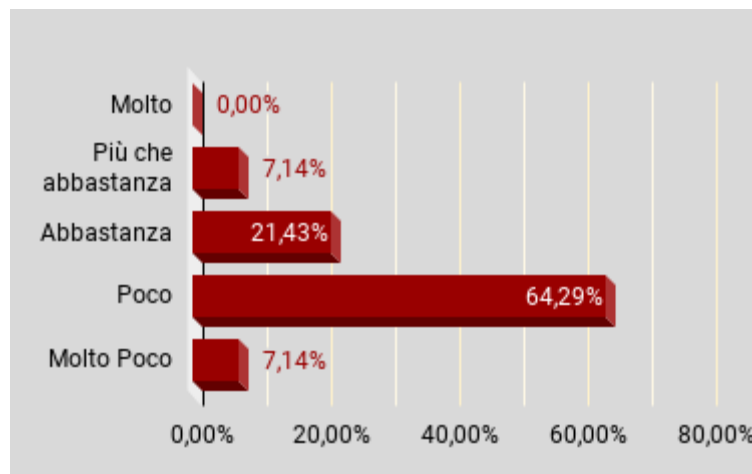
*Opinión de los padres sobre los métodos de protección de la salud adoptados por los niños*



Por otra parte, las opiniones de los padres difieren de las de los maestros en lo que respecta a los sistemas de eliminación de los dispositivos informáticos que protegen el medio ambiente. Más del 64% cree que sus hijos están suficientemente, o más que suficientemente, informados sobre ese comportamiento; mientras que la tendencia vuelve a ser la misma que la de los profesores en lo que respecta al uso (ver Gráfico 23).

### Gráfico 23

*La opinión de los padres sobre el uso de métodos correctos de eliminación del equipo informático por parte de los niños*



Los padres, al igual que los profesores, piensan que los niños son conscientes de que los datos personales distribuidos en Internet pueden ser robados (alrededor del 70% lo piensa); y más del 60% también cree que hace algo para salvaguardarlos. También se han agregado las dos pistas de registro de padres y maestros pertenecientes al instituto privado, obteniendo una única base de datos que representa a los adultos interesados en la institución privada. En este punto, el análisis se distinguió por género para verificar cualquier diferencia en las opiniones de los dos sexos. En general, los adultos de ambos sexos dan respuestas que van en la misma dirección (véase el cuadro 9), con la excepción de la pregunta relativa al conocimiento de los sistemas de eliminación de desechos informáticos, que para el 53% de los adultos de sexo masculino, los niños tienen conocimientos más que suficientes, mientras que para casi el 70% de los adultos, las mujeres, tienen pocos conocimientos. Además, hay que decir que, en este

caso, son las mujeres las que tienen una visión más pesimista, expresando peores juicios hacia el conocimiento que poseen los chicos. Estas opiniones negativas se manifiestan sobre todo en las cuestiones relativas a la protección de la salud, el conocimiento de los sistemas de eliminación de la tecnología de la información y la adopción de métodos de protección de los datos personales. Por otro lado, la visión más optimista de los varones se expresa en términos de conocimiento de la posibilidad de robo de datos personales en Internet (el 91% de los varones adultos están convencidos de que los niños son conscientes de ello, aunque el 55% dice que no hacen nada para protegerse). La comparación, en cambio, con los adultos del instituto técnico-comercial público muestra dos puntos de vista que van en dirección opuesta: el primero es el relacionado con la libertad de uso del teléfono móvil en el aula, que para los adultos del centro público es limitada, sin embargo, para los del privado es considerable. La segunda es que en el conocimiento de los sistemas de eliminación de los dispositivos informáticos, para los varones adultos del instituto estatal es poco, mientras que para los varones adultos del instituto privado es más que suficiente.

**Tabla 23**

*Distribución de los modos de respuesta para hombres y mujeres*

<b>Quesito</b>	<b>Modalità di risposta</b>	<b>Maschi</b>	<b>Femmine</b>
Rischio percepito dagli studenti navigando su internet	Medio-bassa*	52,9 %	61,10%
Libertà di utilizzare il telefono in classe	Medio-alta**	76,50%	61,10%
Tempo dedicato alla navigazione in classe per scopi didattici	Poco***	76,50%	77,80%
Informazione sui programmi per sicurezza dispositivi informatici	Abbastanza****	70,60%	66,70%

Utilizzo dei programmi per sicurezza dispositivi informatici	Poco	56,30%	61,10%
Protezione della salute dall'uso eccessivo del PC	Poco	64,70%	77,80%
Conoscenza di sistemi di smaltimento dei dispositivi informatici	Abbastanza	52,90%	66,70%
Uso sistemi di smaltimento dei dispositivi informatici	Poco	70,60%	77,80%
I dati personali diffusi su internet possono essere derubati	Abbastanza	90,90%	66,70%
Adozione di comportamenti di salvaguardia dei dati personali	Poco	54,50%	61,10%

\* Comprende i valori che vanno da nullo a medio

\*\* Comprende i valori che vanno da medio ad alto

\*\*\* Comprende i valori poco e molto poco

\*\*\*\* Comprende i valori che vanno da abbastanza a molto

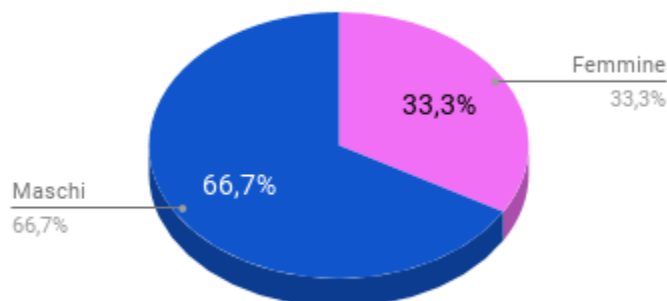
Los alumnos de la institución privada:

El colectivo de alumnos del instituto técnico-comercial privado está compuesto por 27 alumnos de entre 15 y 21 años (edad media 17 años). La diferencia de edad entre los alumnos

del Estado y los del instituto privado (promedio del público: 15/19 años; promedio del privado 5/21 años), se debe a la peculiaridad de las escuelas privadas: la recuperación de los años escolares que pueden haberse perdido y la condición de fracaso escolar de la que proceden todos los alumnos. La muestra está compuesta por un 66,7% de niños y un 33,3% de niñas (ver Gráfico 24).

### Gráfico 24

*Distribución por sexo de los alumnos en la institución paritaria*



### Tabla 24

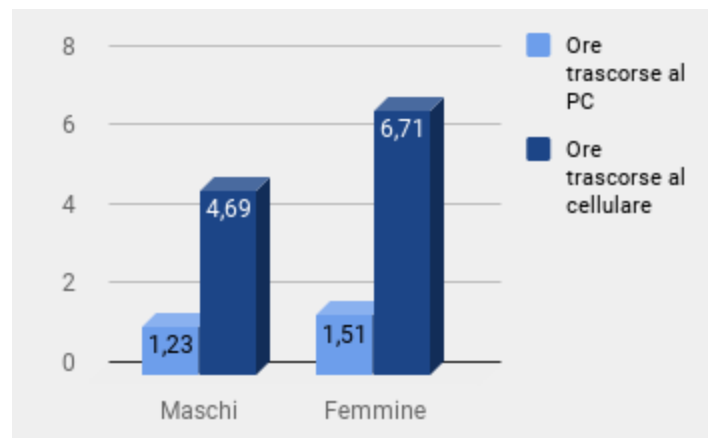
*Número de horas/día pasadas frente a la PC, la tableta y el teléfono móvil*

	N	Minimum	Maximum	Mean	Std. Deviation
Ore_giorno_PC	27	0	6	1,32	1,455
Ore_giorno_tablet	27	0	4	0,45	1,006
Ore_giorno_cellulare	27	0	11	5,36	3,134
Valid N (listwise)	27				

Los datos relativos al número de horas que los niños han declarado pasar frente a un dispositivo electrónico, aunque siguen siendo preocupantes, son inferiores, aunque ligeramente, a los adquiridos en el instituto público. El promedio de horas pasadas frente a un teléfono móvil de 7 horas con picos de 20 se reduce a más de 5 con picos de 11. Para la tableta alcanza casi una hora y para el PC un poco más de una hora. Entre los encuestados sólo hay una persona que dijo que no utiliza su teléfono móvil ni siquiera durante una hora del día y 9 que no utiliza un PC o una tableta. Incluso en la escuela privada hay un alarmante 20% que usa su teléfono móvil durante 10-11 horas al día. Por otro lado, sin embargo, la cifra es más tranquilizadora, ya que otro 20% lo usa moderadamente de 0 a 2 horas. Quiriendo hacer, también en este caso, una distinción por sexo, el resultado es similar al obtenido por el instituto estatal, es decir, las mujeres permanecen frente al teléfono móvil más tiempo que los hombres (una media de casi 5 horas para los hombres frente a una media de casi 7 horas para las mujeres).

### Gráfico 25

*Distribución por sexo de las horas/día pasadas frente a un dispositivo informático*



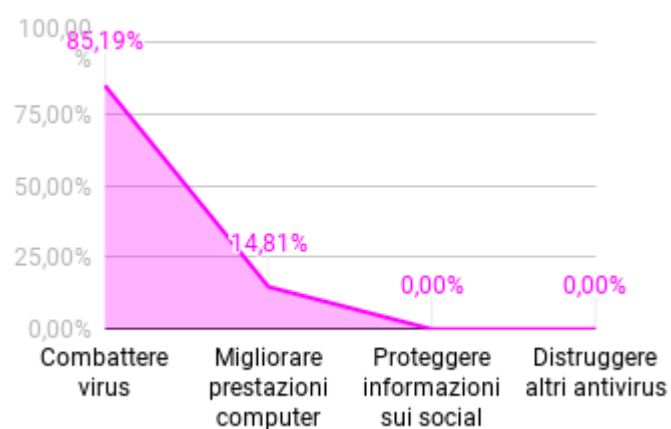
En el primer grupo de preguntas del cuestionario relativo a la protección de los dispositivos de tecnología de la información, los alumnos parecen estar preparados, aunque con algunas más lagunas que sus colegas de la institución estatal. En la primera pregunta "¿Para qué sirve un programa antivirus?" el porcentaje de respuestas correctas es alto, superando el 85%, acercándose así a los resultados obtenidos por los alumnos del instituto estatal. Sin embargo, a



partir de la segunda pregunta, los estudiantes de la institución privada muestran algunas dudas más y los sujetos que conocen perfectamente la definición de virus son 17 de 27 (equivalente al 63%).

## Gráfico 26

*Las respuestas de los alumnos de la institución paritaria sobre la definición de programa antivirus*



Sólo el 59% de los encuestados saben que abrir archivos adjuntos de correo electrónico, aunque los encuentren interesantes, no es recomendable para la protección de su PC. El 55% de los sujetos están informados de que es aconsejable mantener su sistema operativo actualizado con la última versión disponible, de lo contrario los hackers podrían aprovecharse de un fallo o debilidad en el sistema antiguo e infectarlo con un virus. Desciende al 63% el porcentaje de los que saben que una actualización continua del antivirus no significa que la PC sea inmune a las infecciones virales y al 70% el porcentaje de los que saben que el software antivirus preinstalado en la compra no es suficiente para proteger su PC.

### Gráfico 27

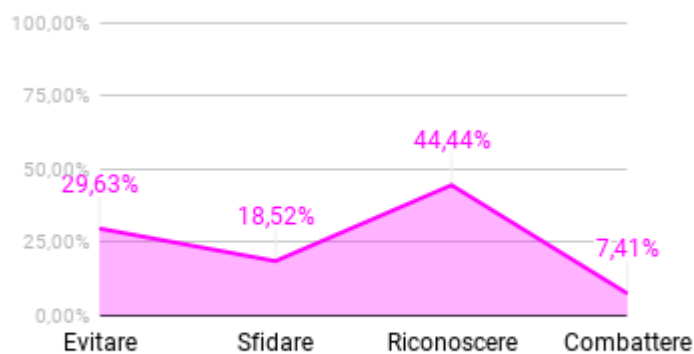
Las respuestas de los alumnos a la pregunta "Mientras el software antivirus esté actualizado ningún virus puede infectarlo"



Por otro lado, en la última pregunta los estudiantes parecen estar mejor preparados, al menos así lo reconoce un 90%, respecto a cómo crear contraseñas seguras. En la primera pregunta de la segunda secuencia relativa a la protección de los datos personales, los alumnos de la institución privada parecen estar un poco confundidos (véase el gráfico 28) y sólo el 44% respondió correctamente.

### Gráfico 28

Las respuestas de los alumnos sobre el primer paso para protegerse de los riesgos cibernéticos



Lo que se desprende de la segunda pregunta de esta serie resulta algo decepcionante, a saber, la existencia de un 33% que desconoce que una vez que el contenido se publica en Internet siempre deja rastro.

El 80%, por otra parte, es consciente de que no es conveniente acceder a sus datos personales desde un ordenador público y casi todos, es decir, alrededor del 93%, son conscientes de los canales de ataque del ciberacoso.

**Tabla 25**

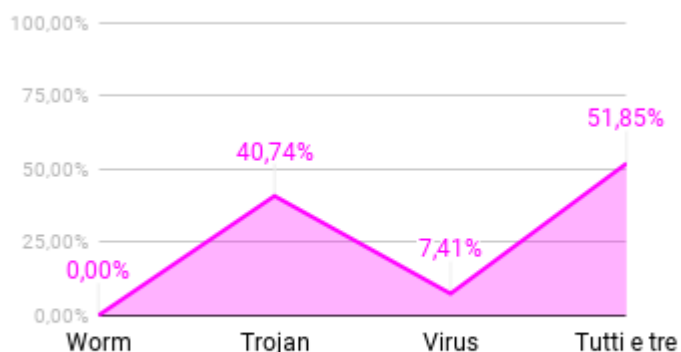
*El acoso cibernético puede ocurrir a través de computadoras, teléfonos móviles y tabletas*

		Frequency	Percent	Valid Percent
Valid	Falso	2	7,4	7,4
	Vero	25	92,6	92,6
	Total	27	100	100

Más confusión crea la pregunta sobre la definición de malware, cuya tasa de respuesta correcta parece casi igual a la obtenida por la institución estatal.

## Gráfico 29

### Definición de *malware*



Como se ha podido comprobar, la cuestión respecto al buen uso de las redes sociales fue contestada de modo diverso. Casi todos los alumnos del grupo de compañeros prefirieron dar una sola respuesta excepto en 7 asignaturas (que corresponden al 26%). Los alumnos alcanzaron una tasa de respuesta correcta con la primera respuesta del 66,7%, mientras que si consideramos también la segunda respuesta, llegamos a casi el 86% (ver Tabla 11). El icono de navegación de incógnito, que aparece en Mozilla Firefox, también fue reconocido por el 66,7% y este porcentaje se eleva a poco más del 70% cuando se le pregunta si es aconsejable utilizar la opción de recordar la contraseña al cerrar el navegador cuando se accede a su correo electrónico desde un ordenador público. Además, el término "phishing" sólo es conocido por el 40,7% de los encuestados y el porcentaje de éstos indica una confusión generalizada sobre la definición.

**Tabla 26**

*Conocimiento de las estrategias de protección*

		Frequency	Percent	Valid Percent
Valid	Un modo con cui le banche tentano di	4	14,8	14,8

	attirare clienti			
	Un metodo per proteggersi da furti d'identità e frodi online	12	44,4	44,4
	Un'e-mail truffa condotta al fine rubare informazioni ed identità	11	40,7	40,7
	Total	27	100	100

**Tabla 27**

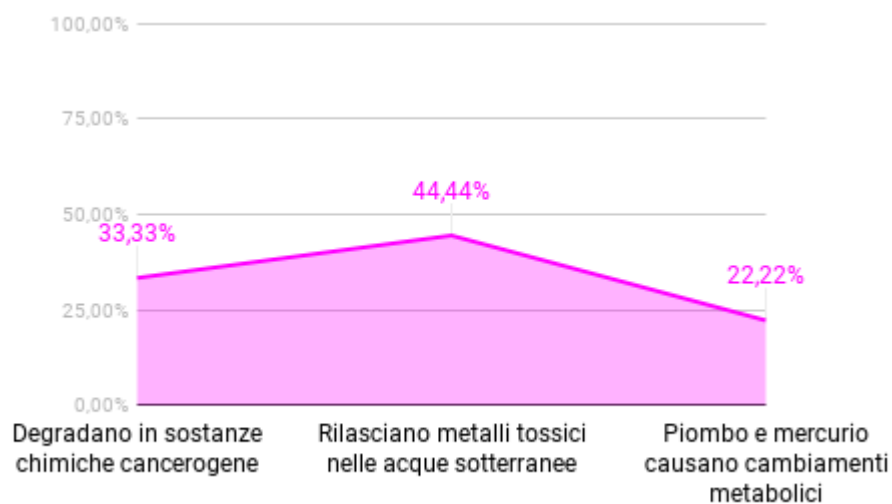
*Protección del medio ambiente*

		Frequency	Percent	Valid Percent
Valid	Ridurre-rispettare-riciclare	13	48,1	48,1
	Ridurre_riutilizzare-riciclare	7	25,9	25,9
	Ridurre-riconsiderare-rispettare	7	25,9	25,9
	Total	27	100	100

La confusión se acentúa en la esfera de la protección del medio ambiente, en particular cuando hay que proporcionar la definición de las tres R de los desechos. La tasa de respuestas correctas se queda en un decepcionante 26%. Por otro lado, en la siguiente pregunta sobre la peligrosidad de los dispositivos electrónicos, los alumnos del grupo de compañeros demostraron estar mejor preparados que sus colegas del instituto público, alcanzando un porcentaje del 44,4% de respuestas correctas.

### Gráfico 30

*Peligros de los dispositivos informáticos*



### Tabla 28

*Definición de desechos electrónicos*

		Frequency	Percent	Valid Percent
Valid	Rifiuti chimici pericolosi	8	29,6	29,6
	Rifiuti derivanti dalla produzione di energia nucleare	7	25,9	25,9
	Apparecchiature elettroniche obsolete	9	33,3	33,3
	Rifiuti ecologici	3	11,1	11,1
	Total	27	100	100

No mejora la situación cuando se les pide a los estudiantes que identifiquen la opción menos útil para la gestión de residuos. De hecho, sólo el 37% puede identificarlo.

**Tabla 29**

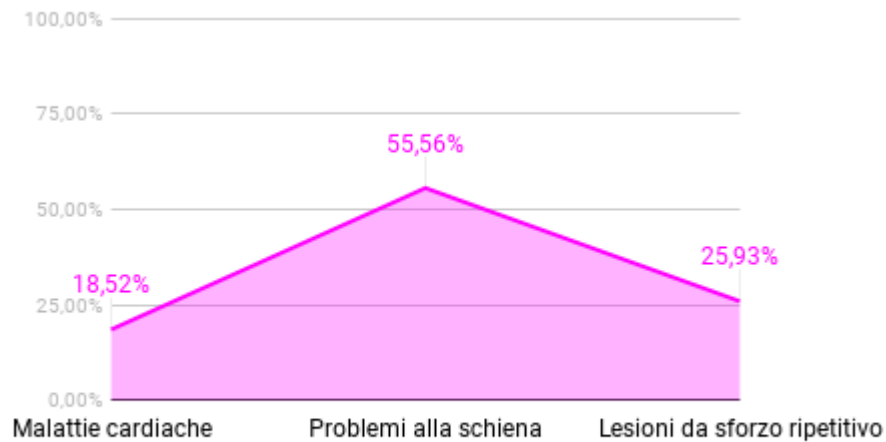
La opción menos útil para la gestión de desechos

		Frequency	Percent	Valid Percent
Valid	Riuso	5	18,5	18,5
	Recupero	12	44,4	44,4
	Smaltimento	10	37	37
	Total	27	100	100

En la penúltima serie de preguntas, aparte de la primera, los estudiantes muestran un cierto grado de preparación. A la primera pregunta, "¿Qué problemas de salud causa el escribir durante horas en el teclado?", una proporción relativamente baja (el 26%) responde correctamente identificando las lesiones provocadas por las tareas repetitivas.

### Gráfico 31

*Problemas de salud causados por escribir durante horas en el teclado*



Por otro lado, más del 80% admite saber que el parpadeo de la pantalla causa fatiga ocular y el 74% sabe que debe sentarse en su escritorio con la cabeza y el cuello en línea con el torso para evitar problemas de espalda. En esta pregunta, sin embargo, el 100% de los alumnos del instituto público respondieron correctamente. Cuando se les preguntó sobre la disposición del monitor en relación con el nivel de los ojos, un tercio de los estudiantes se equivocaron ya que el 33,3% respondió incorrectamente, error que no se detectó entre los estudiantes del instituto público.

### Tabla 30

*Cuando se trabaja en un escritorio, la cabeza y el cuello deben estar alineados con el torso*

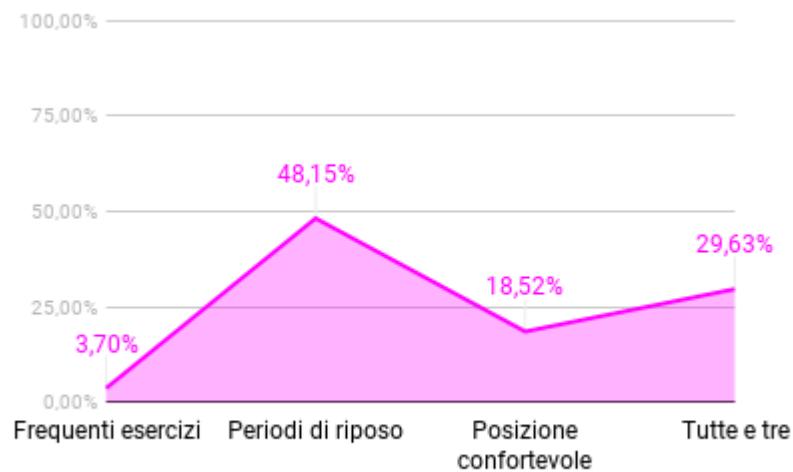
		Frequency	Percent	Valid Percent
Valid	Falso	9	33,3	33,3
	Vero	18	66,7	66,7
	Total	27	100	100



También en este caso, se omitió el estudio de las respuestas correctas vs. incorrectas para las preguntas posteriores, ya que la respuesta queda expresada de alguna manera en el enunciado "todos los mencionados".

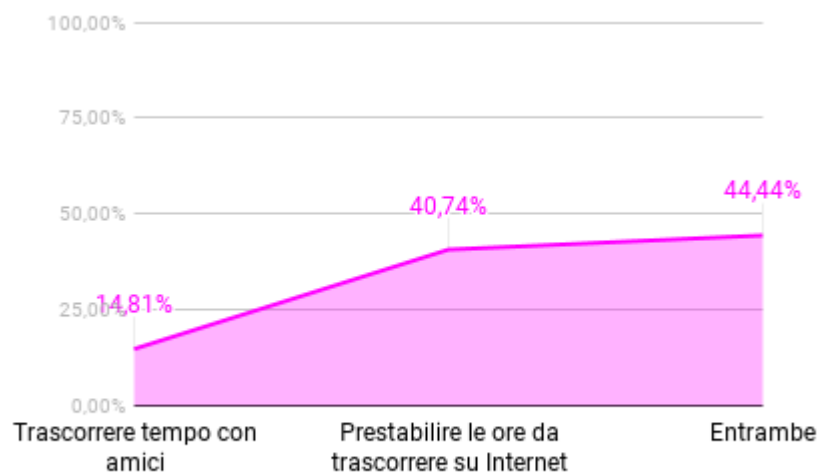
### Gráfico 32

*Cómo reducir los riesgos para la salud causados por el uso prolongado de la computadora*



### Gráfico 33

*Cómo mantener un equilibrio entre el mundo virtual y el real*



En la última serie de preguntas, relativas a la revisión de algunos casos concretos, los estudiantes del grupo de compañeros tuvieron un rendimiento ligeramente superior al de los anteriores. En cuanto a la primera pregunta, es decir, la posibilidad de pagar en línea por una entrada de concierto, la mayoría de los estudiantes (casi el 52%) piensa que la respuesta correcta es pagar con tarjeta de crédito después de verificar la fiabilidad del sitio.

**Tabla 31**

*Pago en línea de una entrada para un concierto*

		Frequency	Percent	Valid Percent
Valid	E' possibile pagare online utilizzando la carta di credito su siti che adottano un certo tipi di protezione	14	51,9	51,9
	Non credo sia possibile pagare online	2	7,4	7,4
	E' possibile pagare online ma occorre conoscere di persona il venditore	5	18,5	18,5
	E' possibile pagare online ma è meglio evitare di farlo	6	22,2	22,2
	Total	27	100	100

Respecto a la pregunta "En qué página web se pueden introducir los datos personales con un cierto grado de seguridad, en la página web oficial del instituto o en un "chat" externo". En comparación con los alumnos de la institución pública entre los que el 90% de ellos respondió

correctamente, mientras que sus compañeros del centro concertada manifiestan tener un comportamiento imprudente en mayor proporción. Baste decir que el 50% de la muestra de estudiantes de referencia estaría dispuesta a introducir sus datos personales en un sitio distinto al ofrecido por la institución de la escuela.

**Tabla 32**

*En qué sitio introducir sus datos personales*

		Frequency	Percent	Valid Percent
Valid	Inserisco i miei dati personali in entrambi i casi	4	14,8	14,8
	Inserisco i miei dati personali solo nel secondo caso	8	29,6	29,6
	Inserisco i miei dati personali solo nel primo caso	15	55,6	55,6
	Total	27	100	100

A la siguiente pregunta: "¿Qué problemas plantea la inclusión de audio, vídeo y fotografías personales en la red?" Aunque la pregunta requeriría habilidades técnicas adicionales, los alumnos del grupo de compañeros consiguen un resultado ligeramente mejor que sus colegas de la institución estatal con una tasa de respuesta correcta de más del 50%.

**Tabla 33**

¿Qué problemas plantea la inclusión de audio, vídeo y fotografías personales en los sitios web?

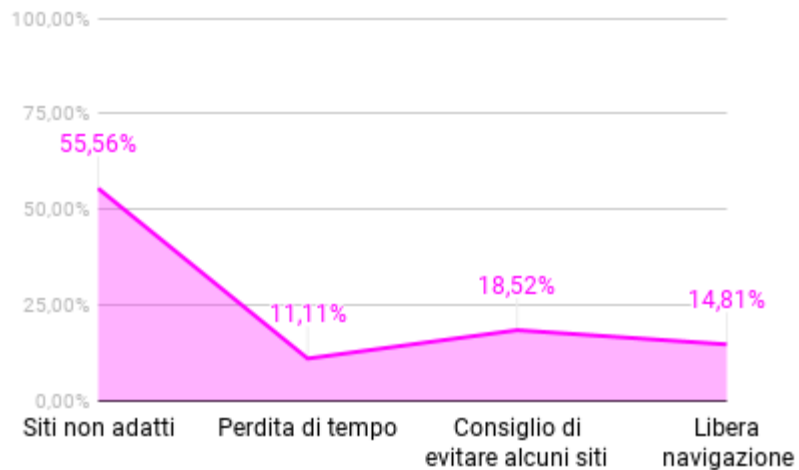
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Rispetto delle clausole d'uso stabilite dagli autori	14	51,9	51,9	51,9
	Titolazione e commento dei materiali da parte di chi accede al sito	4	14,8	14,8	66,7
	Riproduzione dei materiali digitali scaricati	7	25,9	25,9	92,6
	Inserimento/scaricamento di materiali nel sito	2	7,4	7,4	100
	Total	27	100	100	

Sorprende que solo el 50% de los encuestados reconoce estar informados respecto a que publicar un vídeo en internet, requiere el consentimiento de todas las personas que aparecen en el mismo. Cuando se les invita por correo electrónico a una fiesta en una dirección desconocida, los estudiantes dan respuestas contradictorias y sólo el 37% responden que no aceptan. Así, incluso en lo que respecta al consejo que debe dar a su abuelo que recibe un correo electrónico con el logotipo de su banco, sólo el 41% responde que no lo haga y que informe a la policía postal. Cuando se les pregunta si es correcto que un niño de 8 años navegue libremente por Internet, casi el 56% dice que puede no ser una elección segura debido a la posibilidad de encontrarse con sitios inadecuados y, cuando se les pregunta si deben proporcionar sus datos personales en un sitio que ofrece premios, sólo el 59% muestra

un comportamiento igualmente prudente, negándose a hacerlo porque no están seguros de su uso.

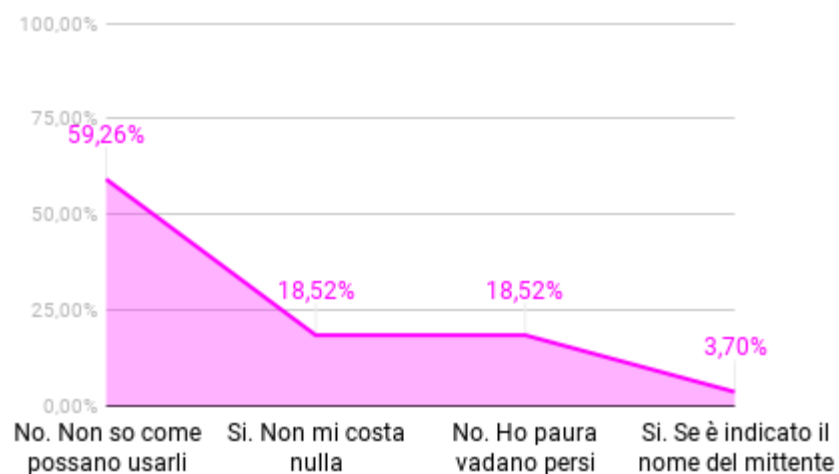
### Gráfico 34

Navegar gratis por Internet para un niño de 8 años



### Gráfico 35

Proporcionar datos personales en un sitio que ofrece premios



También para los alumnos pertenecientes al instituto privado, a fin de determinar si existía algún tipo de relación entre la edad y el tipo de respuesta que se daba a una pregunta un poco más técnica, se hicieron correlaciones bivariadas (entre la variable de edad y la pregunta de interés) y, entre todas las realizadas, se encontró una correlación significativa entre la edad y el phishing en la prueba de Chi cuadrado de Pearson con dos colas en el nivel de significación 0,05. Hubo una asociación positiva entre la respuesta correcta y la edad más alta y entre la respuesta incorrecta y la edad más baja. En lo que respecta a la parte del cuestionario relativa a la evaluación, se obtuvieron los siguientes resultados para los jóvenes del grupo perteneciente a la privada:

- El 74% de los jóvenes declararon que perciben un riesgo medio-bajo mientras navegan por la red;
- Casi el 86% dijo que tenían una libertad media-baja para usar su teléfono móvil en el aula;
- El 74% dice que el tiempo que pasa navegando por el aula con fines educativos es medio-bajo.

### **6.1.3. Comparación de resultados entre centros públicos y concertados**

De la lectura y la comparación de los datos de cada instituto surge un cuadro similar, pero con una marcada superioridad de los resultados obtenidos por los estudiantes que asisten al instituto estatal. De hecho, estos fueron muy competentes en la primera sección del cuestionario:

1. Protección de los dispositivos informáticos (por el término competente entendemos que el promedio de encuestados alcanzó o superó el 75% de respuestas correctas). Con la única excepción del punto relativo a la necesidad de actualizaciones de antivirus, donde se alcanzó un promedio del 65% de respuestas correctas.

Por otra parte, los estudiantes del instituto privado sólo pueden ser considerados competentes en dos de los siete puntos y no alcanzan la competencia en los otros cinco.

- Definición de virus (63%)
- Mal consejo de abrir siempre los archivos adjuntos de los correos electrónicos (59%)
- La actualización del antivirus no garantiza la seguridad (63%)
- Necesidad de actualizar el sistema operativo (55%)
- Caducidad del software antivirus preinstalado (70%)

Lo que tienen en común, negativamente, es que ambos grupos creen que sus dispositivos informáticos son seguros simplemente actualizando el antivirus.

## 2. Protección de los datos personales

También con respecto a la segunda sección, la diferencia entre los resultados de los alumnos de la pública y los de quienes provienen del instituto privado, sigue siendo en gran medida favorable a los de la pública. De hecho, comparando las respuestas, las primeras alcanzan un resultado de competencia en 7 ítems de 9, no alcanzando el nivel del 75% de respuestas correctas en sólo dos ítems:

- Definición de *malware* (51,76%)
- Definición de *phishing* (37,65%)

Los alumnos del grupo de la privada, por el contrario, alcanzan el nivel de competencia en sólo 2 de los 9 ítems, demostrando que no tienen competencia en los otros 7 ítems:

- Reconocer una amenaza a la seguridad de los datos (44%);
- Persistencia de los contenidos publicados en Internet después de su eliminación (67%);
- Definición de malware (51,85%);
- Configuración de seguridad de las redes sociales (26%);
- Definición de phishing (40,7%);
- Reconocer el icono de incógnito (66,7%);
- Recordar la contraseña (70%).

No alcanzan en absoluto el nivel de experiencia en definiciones de *malware* y *phishing*.

### 3. La protección del medio ambiente

Aquí los dos grupos proceden en paralelo con resultados pobres para ambas muestras

- Reducir - Reutilizar - Reciclar (49,4% instituto público; 26% del privado);
- Dispositivos electrónicos peligrosos (33% instituto público; 44,4% del privado);
- Definición de desechos electrónicos (50% instituto público; 33,3% del privado);
- Eliminación, opción menos útil (43% del instituto público; 26% del privado).

Ambos grupos no pueden considerarse competentes en ninguno de los temas de protección del medio ambiente.

### 4. Protección de la salud

Los resultados siguen siendo insatisfactorios en ambas instituciones para casi todos los artículos de la sección. El estado tuvo como resultado un rendimiento ligeramente superior al de sus compañeros, alcanzando el nivel de competencia en 2 de cada 6 ítems en comparación con el otro grupo que sólo alcanza la competencia en 1 de cada 6 ítems.

- Lesiones por esfuerzos repetitivos (38,6% del público; 26% privado);
- Posición ergonómica (74% privado);
- Posición de la pantalla (60% del público; 33% privado);
- Reducir los riesgos del uso prolongado de la PC (38,82% del público; 29,63% privado);



- Equilibrio entre el mundo real y el mundo virtual (57,65% del público; 44,44% privado/concertado).

Todo lo que saben y no de modo muy preciso, es que el parpadeo de la pantalla causa fatiga ocular.

## 5. Casos concretos

Con esta definición nos referimos a las pruebas que evalúan la competencia en una situación. Los alumnos pertenecientes al instituto privado no alcanzaron el valor medio del 75% en ningún ítem. El estado, por otro lado, es competente en 4 de los 6 ítems.

- Autorizaciones para publicar video y audio (47,1% del público; 51% del privado);
- Códigos bancarios de correo electrónico (65% del público; 41% del privado).

En lo que respecta a la institución público, no se encontró ninguna correlación entre las respuestas incorrectas o correctas y la edad de los estudiantes. No se encontró ninguna correlación significativa con la prueba de dos *chi-cuadrado*. En el análisis de los resultados de los estudiantes de la misma edad hubo una asociación positiva, en la definición de *phishing*, entre la respuesta correcta y la edad más alta y entre la respuesta incorrecta y la edad más baja. En la prueba de *chi cuadrado* de Pearson con dos colas, se encontró una correlación a un nivel de significación de 0,05.

**Tabla 34***Relación entre las respuestas y la edad de los estudiantes*

	CONTENUTI	RISPOSTE COMPETENTI NELLA MEDIA RISPETTO AI QUESITI PROPOSTI (público)	RISPOSTE COMPETENTI NELLA MEDIA RISPETTO AI QUESITI PROPOSTI (privado/concertado)
1	PROTEZIONE DEI DISPOSITIVI INFORMATICI	5/7	2/7
2	PROTEZIONE DEI DATI PERSONALI	3/6	2/6
3	PROTEZIONE DELL'AMBIENTE	0/4	0/4
4	PROTEZIONE DELLA SALUTE	2/6	1/6
5	CASI CONCRETI	4/6	1/7

#### **6.1.4 El papel de los profesores y los padres**

Los cuestionarios se administraban a los profesores durante el recreo o al final del horario escolar, y luego por procedimiento aleatorio. Durante la administración de las pruebas, algunos profesores del Instituto Estatal adoptaron una actitud de desconfianza ante la petición de cumplimentación del cuestionario. Esta desconfianza, para algunos, se tradujo en un intento de evitar contestar al cuestionario, citando pretextos como: la prisa, la falta de predisposición tecnológica, las horas de trabajo caducadas. La mayoría de ellos, en su mayoría jóvenes, estaban disponibles e interesados en el resultado de la investigación. Estos

datos parecen ser pertinentes, aunque estén circunscritos numéricamente, ya que en este proceso tan codiciado de digitalización de estructuras y didáctica, el papel del profesor ha asumido un papel primordial y decisivo.

A pesar del proceso de digitalización del Instituto, que cuenta con laboratorios de informática de última generación, algunos profesores (pocos, de hecho) parecen querer rechazar el papel, que les correspondería por definición, de "barqueros" para el desarrollo de la identidad adulta de sus alumnos (Ammaniti, Tambelli, Zavattini, Vismara y Volpi, 1999). En comparación con el Modelo de Aceptación de Tecnología (TAM) (Davis, Bagozzi y Warshaw, 1989), todos los factores que influyen en el uso o no de una nueva tecnología están, según las respuestas de algunos profesores, prácticamente ausentes. El TAM, de hecho, incluye entre ellos: la utilidad percibida del uso, la actitud, la facilidad de uso. Y también el concepto de "Intención" al que se refiere Ajzen (1991). El primer cuestionario, el más breve, fue concebido, de hecho, para ser administrado a los padres y a las figuras que están en contacto directo con la formación educativa de los adolescentes, como los profesores, a fin de tener su opinión subjetiva sobre la conciencia de los estudiantes en el campo de la seguridad informática. "El uso de las tecnologías de la información, de hecho, si por un lado ha traído y está trayendo un gran progreso en el conocimiento, por otro lado puede ser un factor de riesgo relevante en fases de la vida, como la adolescencia, en la que la estructura de la personalidad del individuo se encuentra en una fase de consolidación y expansión" (Ammaniti et al., 1999). Por lo tanto, el adolescente de hoy se presenta al desafío evolutivo que representa la adolescencia con ese "bagaje tecnológico" que puede ser una ayuda para superar las diversas tareas evolutivas, o puede representar una carga, o un peligro real.

En particular, en la adolescencia, el uso indebido de esta tecnología puede representar un refugio y conducir al aislamiento, o al compromiso de la relación con los demás, o incluso a la pérdida de contacto con la realidad. Si, de hecho, esta modalidad de alejamiento de la realidad no asume un carácter transitorio sino que se transforma en hábito, el estilo de vida se caracterizará inevitablemente por la dependencia y el adolescente se encontrará viviendo, de manera disociativa, una realidad virtual paralela, caracterizada por relaciones sociales, intercambios comunicativos, aperturas relacionales que poco tienen que ver con la vida cotidiana de la realidad externa" (Kuss, Griffiths, & Binder, 2013).

### **6.1.5. Triangulación de la evaluación**

Mediante la comparación de los resultados de los cuestionarios aplicados a las familias, al profesorado y a los técnicos de laboratorio, hemos podido conocer su opinión sobre los conocimientos adquiridos por el alumnado e hijos/as. De todo lo cual se desprende que tanto el profesorado como las familias piensan que el alumnado tiene suficientemente claro el riesgo que corre navegando en Internet, de hecho, el 70% de los encuestados les atribuye un nivel dominio Medio-Alto. Los técnicos de laboratorio, en cambio, se encuentran en una posición opuesta creyendo que no tiene ninguna conciencia.

Los encuestados están de acuerdo, en un nivel medio, acerca de la libertad del alumnado para utilizar los teléfonos móviles en clase. En cuanto a su opinión sobre el tiempo que dedican a Internet con fines educativos, esta vez es el profesorado el que se desmarca del grupo afirmando, en un 71,4%, que el alumnado lo utiliza poco o muy poco. Las familias, en un 51,4%, están de acuerdo con los técnicos cuando afirman que es suficiente o más que suficiente. En cuanto a la pregunta relacionada con el conocimiento del alumnado sobre los programas de seguridad informática, la respuesta de las familias difiere y un 51,4% piensa que conocen la temática, frente a poco o muy poco de los técnicos y del profesorado.

En cambio, la muestra de las familias se asemeja al grupo cuando se les pregunta que si conociendo los programas de seguridad los utilizan. En los tres grupos las respuestas se concentran en poco o muy poco. De los resultados se desprende, además, que el alumnado, según la opinión de los adultos de su entorno, no son capaces de proteger su salud del uso excesivo del ordenador. En cuanto al conocimiento de los comportamientos de eliminación de los dispositivos informáticos y su aplicación, todos los sujetos convergen en muy poco. En cambio, los resultados algo más alentadores provienen de los datos relacionados con la protección de los datos personales, en los que parece que el alumnado es consciente de la posibilidad de que les roben sus datos y para evitarlo ponen en práctica acciones de protección de sus contenidos.

**Tabla 35***Comparación de las respuestas de los distintos agentes*

	DOCENTI	GENITORI	GENITORI E DOCENTI	TECNICO DI LABORATORIO
Che grado di rischio percepiscono di correre, gli studenti, navigando in Internet	Medio-alto 61,9%	Medio-alto 82,9%	Medio alto 70%	Nulla
Che libertà hanno, gli studenti, di utilizzare il cellulare in classe	Medio-alto 57,1%	Medio-alto 57,1%	Medio basso 60,7%	Medio
Quanto tempo, gli studenti, dedicano alla navigazione in Internet per motivi didattici	Poco o molto poco 71,4%	Abbastanza o più che abbastanza 51,4%	Poco o molto poco 53,6%	Abbastanza
Gli studenti, sono informati dell'esistenza di programmi per la sicurezza dei dispositivi informatici	Poco o molto poco 57,2%	Abbastanza 51,4%	Poco 37,5% Abbastanza 39,3%	Molto poco
...se conoscono i programmi sulla sicurezza informatica, secondo te, li utilizzano	Poco o molto poco 57,2%	Poco 40% abbastanza 40%	Poco o molto poco 58,9%	Molto poco
Gli studenti, sanno proteggere la loro salute dall'uso	Poco o molto poco 76,2%	Poco o molto poco 74,3%	Poco o molto poco 82,1%	Molto poco

eccessivo del computer				
Gli studenti, conoscono quei comportamenti di smaltimento dei dispositivi informatici che proteggono l'ambiente	Poco o molto poco 90,5%	Poco o molto poco 71,5%	Poco o molto poco 78,6%	Molto poco
...se li conoscono, secondo te, li mettono in pratica	Poco o molto poco 95,2%	Poco o molto poco 71,5%	Poco o molto poco 80,4%	Molto poco
Gli studenti, sanno che i dati personali diffusi su internet possono essere rubati	Abbastanza o molto 85,7%	Abbastanza 42,9%	Abbastanza 44,6%	Abbastanza
... se lo sanno, mettono in pratica dei comportamenti che salvaguardano i loro dati personali?	Poco o molto poco 76%	Abbastanza o più che abbastanza 51,4%	Poco o molto poco 55,4%	Abbastanza

## **CAPÍTULO VII**

### **Conclusiones generales**

#### **7.1. Consideraciones finales**

Este trabajo ha centrado su atención en las habilidades digitales, relacionadas con la seguridad en línea, que poseen los estudiantes que asisten a la escuela secundaria, estatal y privada en Italia. Estas habilidades fueron entendidas como habilidades cognitivas, socio-éticas y prácticas. Lamentablemente, los niveles de competencia registrados fueron, en general, casi mediocres por parte de los alumnos del estado y casi pobres por parte de los alumnos del grupo pertenecientes al instituto privado. En particular en la escuela estatal, se encontró un nivel de competencia suficiente en general en los casos prácticos y en la evaluación de la competencia en la situación, con un promedio de 5 de cada 7 ítems en los que se alcanzó el nivel de competencia requerido (75%). En la misma escuela los alumnos también demostraron un nivel de competencia justo en la protección de los dispositivos informáticos con 4 de cada 6 respuestas competentes.

Por otra parte, los datos sobre la protección del medio ambiente en los que no se alcanzaron los valores de competencia en ningún punto son preocupantes. Asimismo, se evaluaron los resultados relativos a la protección de la salud, en los que se alcanzó el nivel de competencia requerido en promedio sólo en 2 de los 6 puntos. El nivel se reduce más con respecto al rendimiento de los compañeros, resultados que nos llevan a evaluarlos como poco competentes. Estos resultados se compararon con los datos de encuestas anteriores realizadas en Italia utilizando el mismo instrumento de evaluación diseñado por Calvani y sus colaboradores. Las conclusiones de una de estas encuestas, realizada por el propio Calvani y de la que se informa a continuación, convergen significativamente con muchos de los datos que hemos reunido, lo que nos lleva a pensar que las acciones de alfabetización informática, al menos en lo que respecta a la seguridad, no han colmado suficientemente las lagunas de conocimiento identificadas por las encuestas anteriores.

Las puntuaciones resultantes, al menos en los institutos que constituyeron la muestra de estudio correspondientes a los conocimientos prácticos, son de buen nivel, mientras que van disminuyendo progresivamente en relación con los temas relativos a la comprensión de los conceptos y actitudes de precaución relacionados con la competencia de la seguridad en línea (Calvani, Fini, Ranieri, & Picci, 2012). Los estudiantes de esta encuesta anterior, como los de nuestro estudio, "no cuestionan espontáneamente la fiabilidad de la información de Internet" (Calvani et al., 2012b). A pesar de la facilidad de acceso a la Internet y de las muchas horas que los estudiantes afirman pasar en línea (en promedio 7 horas, con un máximo del 20% que afirma navegar durante más de 10 horas al día), el rendimiento de los estudiantes, en promedio, se mantiene en un nivel de competencia medio-bajo. No había diferencias significativas en el rendimiento de los estudiantes de ambos sexos.

La competencia se eleva al nivel, en cambio, con respecto a la investigación de Calvani, en lo que se refiere al ciberacoso, pero sólo en el instituto estatal. En este sentido, casi todos los estudiantes muestran que conocen los canales de difusión del ciberacoso (estado 98,8%; igual 93%), pero sólo los estudiantes del estado consideran inaceptable burlarse de los defectos de los demás a través de las redes sociales (estado 97,6%). Menos determinados en este punto parecen, de hecho, los alumnos del grupo de compañeros con un modesto 51,9% que consideran el hecho inaceptable, mientras que el resto del grupo de clase piensa que no hay nada malo en tal comportamiento (22,2%), junto con otro 22,2% que no aprueban la actitud, pero aún así participan en la broma. Del estudio realizado surge una imagen de estudiantes



suficientemente competentes en habilidades prácticas, pero aún no competentes en un nivel más alto de conciencia ética y social, prudencia y privacidad. Los datos publicados en el artículo: ¿Son las generaciones jóvenes en la escuela secundaria digitalmente competentes? Un estudio sobre los adolescentes italianos (Calvani et al., 2012). De la misma manera, los datos procedentes de la encuesta sobre una muestra de estudiantes chinos seleccionados al azar en la ciudad de Ningbo (Li & Ranieri, 2010) son similares. También en este caso, el rendimiento de los estudiantes fue en general suficiente pero no bueno o excelente. Los resultados mostraron el mismo predominio de respuestas no plenamente satisfactorias en el área ética y cognitiva. Al igual que en el primero, también en este estudio, realizado en China, los mejores resultados se obtuvieron en el área tecnológico-práctica. La conclusión compartida es que los llamados nativos digitales no son necesariamente "conocedores de la red". (Lorenzo, G. y Dziuban). El presente estudio llega a la reflexión de que los resultados de los alumnos de las dos escuelas diferentes reflejan el grado de éxito académico de los alumnos de las dos escuelas. Mejores resultados en la escuela estatal y resultados insuficientes en el instituto privado. Una brecha similar surge de otros estudios (Calvani y otros, 2012; Li y Ranieri, 2010) que encontraron diferencias en los resultados entre las escuelas de formación profesional y las escuelas secundarias. De hecho, estas lagunas, que se ponen de manifiesto en el análisis de los datos, parecen ser difíciles de comprender, a la luz de toda la bibliografía que se ha desarrollado en torno al tema en los últimos años y a la luz de las numerosas encuestas realizadas en toda Italia (Calvani et al., 2012) y en muchos otros países (Kvavik, 2005; Li & Ranieri, 2010). La brecha tangible entre las competencias de los alumnos procedentes de diferentes escuelas (en nuestro caso estatales e iguales) confirma el papel central y fundamental de la Escuela en las competencias de los alumnos. A ello se suman las opiniones de profesores y padres que temen, con razón, que sus alumnos o hijos no sean capaces de defender su salud frente al uso excesivo de Internet (82,1% adultos), que desconozcan esos comportamientos de eliminación de los dispositivos informáticos que protegen el medio ambiente (78,6% adultos) y que, si los conocen, sin embargo, no sean capaces de ponerlos en práctica (80,4%). Todas las aprehensiones confirmadas por el técnico de laboratorio que puede observar el comportamiento de los estudiantes de forma directa y constante. En cuanto a las opiniones de los adultos sobre las demás competencias que poseen o no los alumnos, las respuestas de los profesores y los padres se han fragmentado de manera insignificante, revelando una falta de comprensión de la cuestión o una ignorancia extrema sobre el tema. El análisis de los datos confirma la inevitable necesidad de:

- Desarrollar proyectos en el entorno escolar destinados a la seguridad de los alumnos en la Internet, creando materiales educativos destinados a desarrollar la competencia de la seguridad en línea. Necesariamente en italiano;
- Considerar la seguridad electrónica y la competencia digital como parte del programa de estudios de la escuela y enseñar sus contenidos como materias autónomas no incluidas en otras asignaturas y dejadas, por tanto, a la discreción del profesor de matemáticas o informática individual;
- Sensibilizar a los estudiantes, profesores y padres sobre la necesidad de un cambio en la enseñanza ante la digitalización de la escuela italiana;
- Desarrollar una actitud crítica en los estudiantes hacia un uso responsable de las TIC;
- Entender las competencias digitales como parte integral del aprendizaje permanente de los ciudadanos del mundo.

Es necesario evaluar continuamente los riesgos, las oportunidades y las formas de utilizar los recursos en línea. De hecho, compartimos la reflexión de Bernhard Jungwirth, coordinador de Saferinternet.at, quien sostiene que los jóvenes usuarios de Internet no son capaces de superar el estancamiento que los ve, por un lado, suficientemente conscientes de los riesgos y la falta de fiabilidad de las redes sociales pero, por otro lado, dependientes de ellas para desarrollar relaciones sociales y alcanzar recursos culturales e informativos. Una sugerencia, adoptada por algunas instituciones educativas estatales y no estatales, fue acreditar su escuela a European Schoolnet, la asociación que ha desarrollado una etiqueta de seguridad electrónica que los maestros y otros profesionales pueden utilizar para evaluar la forma en que se enfrentan a los problemas de seguridad en línea dentro de su escuela. La etiqueta *eSafety* es un servicio de acreditación y apoyo en toda Europa para que las escuelas revisen sus prácticas de seguridad electrónica en función de las normas acordadas internacionalmente. Al presentar pruebas del desarrollo y la práctica de la competencia en materia de seguridad en línea, las escuelas pueden ser acreditadas como una escuela certificada en seguridad electrónica. Sin embargo, el sitio no está traducido a los diferentes idiomas y, por lo tanto, requiere un buen conocimiento del inglés por parte de los estudiantes y profesores.

El análisis de los resultados obtenidos en esta encuesta revela, de hecho, la conciencia, tanto de los padres como de los maestros, de los problemas y riesgos relacionados con la seguridad en línea. La dirección de la escuela también ha abordado el problema de la seguridad en línea, con circulares y directivas que exigen que los estudiantes tengan una autorización para entrar en Internet. Además de esto, el profesor y el técnico de laboratorio están constantemente monitoreando la situación. Bajo ninguna circunstancia, entonces, se les permite entrar en ninguna red social a través de los ordenadores de la escuela. Otro punto en el que hay que centrar la atención es el papel de los padres que no participan en ninguna actividad de formación y que, por consiguiente, no pueden dirigir el comportamiento de sus hijos en línea hacia formas seguras. Aunque los padres temen los riesgos que sus hijos pueden correr en línea, dejan que sus hijos naveguen solos a casa en Internet. Por lo tanto, los padres parecen estar entre los principales grupos destinatarios de posibles nuevos recursos de asesoramiento y orientación en materia de seguridad. Una encuesta realizada hace unos años muestra que más del 45% de los recursos encontrados en línea provienen de los Estados Unidos, seguidos por el 16% del Reino Unido y el 12% de Finlandia. Sería apropiado dar lugar a nuevas percepciones sobre la posible dificultad de utilizar y comprender los recursos del idioma inglés por parte de los usuarios italianos. Una eventualidad positiva, podría representar en Italia otra barrera al desarrollo general de las habilidades de seguridad en línea.

La hipótesis del estudio es una preparación insuficiente, por parte de los estudiantes, en cuanto a los problemas de seguridad en línea. Además, se supone que no existen instrumentos de evaluación compartidos y que se retrasan las acciones efectivas dirigidas a la capacitación de todos los actores del sistema escolar. Cabe señalar, en relación con los profesores que, aunque animados a formarse por las políticas gubernamentales, se ven obligados a enfrentarse a otro elemento disuasorio, a saber, el conocimiento del idioma inglés, que no siempre poseen todos. Esta competencia parece más indispensable que nunca para poder aprovechar los inmensos recursos de formación propuestos por la Red. La propuesta es compartir este sistema de evaluación con otras escuelas, a fin de comprender el nivel de competencia relacionado con la seguridad en línea que poseen los estudiantes en una zona determinada (provincia/región) e intervenir de manera informada y específica en las lagunas de conocimiento de los estudiantes identificadas por el cuestionario. Las opiniones y evaluaciones de los profesores y los padres serán otros puntos de vista que se evaluarán para comprender el fenómeno.

## 7.2. Propuesta

Los resultados de este trabajo, junto con el análisis de los estudios publicados en la literatura nacional e internacional, nos han proporcionado una visión desigual y fragmentada de los problemas de seguridad en línea en Italia. De ahí la necesidad de contar con datos fiables e indicadores normalizados para medir la competencia en materia de seguridad. Como ya hemos dicho, creemos que la educación escolar tradicional puede integrarse con las nuevas tecnologías en línea de manera rentable y provechosa para ambos sectores. La cuestión de la seguridad en línea es un problema político que aún no ha sido resuelto completamente por la Ley de la Buena Escuela (Baldacci et al., 2016). Las variables que deben abordarse son muchas y están en constante evolución. En nuestra opinión, requiere una vigilancia constante y nuevas investigaciones profundas, en todo el territorio. Desde el punto de vista educativo, el camino a seguir es hacia el aprendizaje a lo largo de la vida mediado por instituciones educativas.

El proyecto que proponemos es una plataforma libre para compartir el conocimiento y la cultura participativa, al estilo de la wikipedia. Sin embargo, se requerirán diferentes licencias de usuario y niveles de autorización. La plataforma parte de la evaluación de la competencia en línea (según el marco creado por Calvani). El acceso se considera libre en el sentido de que puede ser utilizado por todos, pero con licencias de usuario para la modificación y actualización del contenido. Ese contenido sólo puede ser modificado por expertos calificados en la materia. El idioma elegido sería, por supuesto, el inglés, pero con la posibilidad de traducciones por profesores cualificados también acreditados por el sistema. Estos profesionales podrán acordar cambios y actualizaciones en un foro dedicado a ellos.

La contribución a la formación y a la acreditación son voluntarias. Cada escuela puede contar con su propio animador digital para unirse al proyecto. Los resultados se introducirán en una base de datos estadísticos que ofrecerá una visión lo más precisa y completa posible, dada la participación de todas las escuelas (escuelas secundarias) repartidas por el territorio que serán alentadas por las administraciones a unirse al estudio. Los datos se harán públicos para que se pueda intervenir e investigar más a fondo en este campo. El análisis será también un análisis comparativo que identificará las mejores estrategias de enseñanza que han dado los mejores resultados.

## REFERENCIAS BIBLIOGRÁFICAS

- Ajzen, I. (1991). The theory of planned behavior: organizational Behavior and Human Decision Processes, 50, 179-211. Retrived from [http://cadmus.eui.eu/handle/1814/19794](http://doi.org/10.1016/0749-5978(91)90020-Ambrosini, M. & Caneva, E. (2011). The Embodiment of Tolerance in Discourses and Practices Addressing Cultural Diversity in Italian Schools. University of Mila. Retrived from <a href=)
- American Library Association. (2000). Association of college and research libraries (ACRL). Information Literacy Competency Standards for Higher Education. Chicago.
- Ammaniti, M., Tambelli, R., Zavattini, G. C., Vismara, L. & Volpi, B. (1999). Attaccamento e funzione riflessiva in adolescenza. *Psicologia Clinica Dello Sviluppo*, 3(1), 155-176.
- Astorri, R. (2000). Legge 10 marzo 2000, n. 62" Norme per la parità scolastica e disposizioni sul diritto allo studio e all'istruzione"(vedi commento di F. Freni). *Quaderni di diritto e politica ecclesiastica*, 8(2), 603-605.
- Baccini, M. (2008). Multiple imputation for missing data: a brief introduction. *Epidemiologia e prevenzione*, 32(3), 162. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/18828554>
- Baker, F. (2017). *Close reading the media: literacy lessons and activities for every month of the school year*. New York: Routledge.
- Baldacci, M., Brocca, B., Frabboni, F. & Salatin, A. (2016). *La buona scuola: sguardi critici dal documento alla legge*. Milano: FrancoAngeli.
- Barone, C. (2005). La faiblesse de l'instruction privée en Italie: un paradoxe? *Sociétés contemporaines*, 59-60(3), 97-119. doi:10.3917/soco.059.0097.

- Bawden, D. & Robinson, L. (2002). Promoting literacy in a digital age: approaches to training for information literacy. *Learned Publishing*, 15(4), 297-301. doi:10.1087/095315102760319279.
- Biasi, V. (2017). Didattica digitale e relazione educativa virtuale: una indagine empirica sull'efficacia dei sistemi audio-video nella didattica on-line per la scuola secondaria di secondo grado e l'università. *FORMAZIONE & INSEGNAMENTO. Rivista Internazionale Di Scienze Dell'Educazione E Della Formazione*, 15(1), 67-80.
- Bocci L., Muratore M.G., Signore M. & Tagliacozzo G. (2002), The interviewer effect on the Data Collection of Sensitive Questions. *Atti della XLI Riunione Scientifica della SIS, Sessione Data Quality and accuracy*, pp299-302.
- Bossi, G., & Scellato, G. (2005). *Politiche distrettuali per l'innovazione delle regioni italiane. Promosso dal Ministro per l'Innovazione e le Tecnologie*, Madrid: COTEC, Fondazione per l'Innovazione Tecnologica.
- Bove, G. (2010). *Metodi per l'analisi di Skew-Symmetry in Scaling multidimensionale asimmetrico: classificazione come strumento per la ricerca*. New York: Springer, Berlino, Heidelberg.
- Bruni, A. & Gobo, G. (2005). Qualitative research in Italy. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 6(3), Art. 41. Retrived from <http://nbnresolving.de/urn:nbn:de:0114-fqs0503410>
- Buccoliero, E. & Maggi, M. (2017). *Contrastare il bullismo, il cyberbullismo e i pericoli della rete: manuale operativo per operatori e docenti, dalla scuola primaria alla secondaria di 2° grado*. Milano: FrancoAngeli.
- Buckingham, D. (2006). *Children and new media*. (pp. 75-91) SAGE Publications Inc. doi:10.4135/9781446211304.n3. Retrieved from <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84951177855&partnerID=40&md5=3ab3ea6782a53644ab6da5be1ae64518>
- Buckingham, D. (2005). *The media literacy of children and young people: a review of the research literature*. London: Ofcom. Retrived from: <http://www.ofcom.org.uk>

- Buckingham, D., Banaji, S., Carr, D., Cranmer, S., & Willett, R. (2005). *L'alfabetizzazione mediatica di bambini e giovani: una rassegna della letteratura di ricerca*. London: London Knowledge Lab, University of London.
- Calvani, A., Fini A. & Ranieri M. (2010). *La competenza digitale nella scuola: modelli e strumenti per valutarla e svilupparla*. Trento: Edizioni Erickson.
- Calvani, A., Fini, A. & Ranieri, M. (2011). *Valutare la competenza digitale: Prove per la scuola primaria e secondaria*. Trento: Edizioni Erickson.
- Calvani, A., Fini, A. & Ranieri, M. (2014). La competenza digitale nella scuola. Modelli, strumenti, ricerche. *Italian Journal of Educational Research*, (5), 9-21.
- Calvani, A., Fini, A. & Ranieri, M. (2010). *La competenza digitale nella scuola. Modelli e strumenti per valutarla e svilupparla*. Trento: Erickson
- Calvani, A., Fini, A., Ranieri, M., & Picci, P. (2012). Are young generations in secondary school digitally competent? A study on Italian teenagers. *Computers & Education*, 58, 797–807. doi:10.1016/j.compedu.2011.10.004 Cambridge: Cambridge University Press.
- Calvani, A. & Menichetti, L. (2014). Valutazione della competenza digitale: che cosa fare per la scuola primaria. *Journal of Educational, Cultural and Psychological Studies (ECPS Journal)*, (10), 285-303.
- Calvani, A. & Rotta, M. (2000). *Fare formazione in internet: Manuale di didattica online*. Trento: Erickson
- Calvo, M., Ciotti, F., Roncaglia, G. & Zela, M. A. (2003). *Internet 2004: manuale per l'uso della Rete*. Bari: Laterza.
- Castoldi, M. (2010). La valutazione delle istituzioni educative: approcci a confronto. *Rassegna Italiana Di Valutazione*, 14(46).
- Cinque, D. (2012). La media education come nuova forma di cittadinanza nella società della conoscenza. (Tesi dottorale. Università La Sapienza, Roma). Retrived from <http://padis.uniroma1.it/handle/10805/1581>
- Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35(8), 982-1003

- De Feo, A. & Pitzalis, M. (2014). Arrivano le LIM! rappresentazioni e pratiche degli insegnanti all'avvio della scuola digitale. *Scuola Democratica*, 14(1), 97-116.
- Decaro, M. (2011). *Dalla strategia di lisbona a europa 2020*. Roma: Fondazione Adriano Olivetti.
- Presidenza del Consiglio dei Ministri. (2000). Dipartimento della funzione pubblica. Piano di Azione di e-government, 2000. Retrived from [www.provincia.torino.gov.it](http://www.provincia.torino.gov.it)
- Dewdney, A. K. (1985). Computer Recreations-A Core War bestiary of viruses, worms and other threats to computer memories. *Scientific American*, 252 (3), 14-23.
- Di Lampedusa, G. T. (2002). *Il gattopardo*. Milano: Feltrinelli.
- Domenici, G. (2017). Il contributo della nuova formazione docente per contrastare bullismo e cyberbullismo. *Journal of Educational, Cultural and Psychological Studies* (ECPS Journal), 16, 11-16.
- Endler, N. S. & Parker, J. D. (1990). Multidimensional assessment of coping: a critical evaluation. *Journal of Personality and Social Psychology*, 58(5), 844-856.
- Eshet-Alkalai, Y. (2004). Digital literacy: a conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia*, 13(1), 93-106.
- EU. (2006). *Competenze chiave per l'apprendimento permanente*. Bruxelles: UE.
- EU (2006). Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning (2006/962/ EC). *Official Journal of the European Union*, L 394, 10-18.
- Ferrari, A. (2012). Digital competence in practice: an analysis of frameworks. Seville: Joint Research Centre, Institute for Prospective Technological Studies. <http://dx.doi.org/10.2791/82116>
- Ferrari, A. (2013). DIGCOMP: A *Framework for Developing and Understanding Digital Competence in Europe*. Luxembourg: Publications Office of the European Union. doi:10.2788/52966
- Ferri, P. (2005). *E-learning: didattica, comunicazione e tecnologie digitali*. Firenze: Le Monnier.



- Fortini, M., Scanu, M. & Signore, M. (2000). Use of indicators from data editing for monitoring the quality of the survey process: The Italian information system for survey documentation (SIDI). *Statistical Journal of the United Nations Economic Commission for Europe*, 17(1), 25-35.
- Freni, F. (2003). Scuole paritarie privato-confessionali e sistema nazionale di istruzione (osservazioni a corte cost., sent. n. 42 del 2003). *Quaderni Di Diritto E Politica Ecclesiastica*, 11(3), 735-746.
- Gapski, H. (2008). Alcune riflessioni sulla digital literacy. *TD-Tecnologie Didattiche*, 43(1), 23-25.
- Gasser, U., Maclay, C. M. & Palfrey, J. G. (2010). *Working towards a deeper understanding of digital safety for children and young people in developing nations*. Berkman Center Research Publication, (2010-7), 10-36.
- Ghirardini, P. G. & Pellinghelli, M. (2001). *Piccole scuole crescono: scuola non statale e scuola statale viste con gli occhi di chi sceglie*. Milano: Franco Angeli.
- Giannatelli, R. (2001). La «Media education» nella scuola: perché, come, che cosa insegnare dei média. *Orientamenti Pedagogici*, 48-2 (284), 281-286.
- Gilster, P. (1998). *Digital literacy*. New York: John Wiley & Sons.
- Goethe, J. W. (2011). *Le affinità elettive*. Milano: Feltrinelli.
- Gómez, J. I. A. & Iania, A. (2013). Media education in Europa. *Aularia: Revista Digital De Comunicación*, 2(1), 43-55.
- Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.
- Himanen, P. (2003). *L'etica hacker e lo spirito dell'informazione*. Milano: Feltrinelli.
- Presidenza del consiglio dei Ministri. Dipartimento per l'innovazione e le tecnologie: ufficio studi. (2003). *Rapporto innovazione e tecnologie digitali in Italia*. Roma: Istituto poligrafico e Zecca dello Stato S.p.A. Retrieved from <http://data.theeuropeanlibrary.org/BibliographicResource/3000106688347>

- Ito, T., Zhang, M., Robu, V., Fatima, S., Matsuo, T. & Yamaki, H. (2010). In Ito T. (Ed.), *Studies in computational intelligence: Preface*. Retrieved from <https://www.scopus.com/inward/record.uri?eid=2-s2.0-78049240706&partnerID=40&md5=e6a602b1592521f0b350edf3d24ba176>
- Jacques, G. (2001). *L'éducation aux médias-les controverses fécondes*. Paris: Hachette.
- Jenkins, H. (2010). *Culture partecipative e competenze digitali: media education per il XXI secolo*. Milano, Guerini e Associati.
- Jenkins, H. & Lacasa, P. (2010). Learning in a participatory culture: a conversation about new media and education. The Official Weblog of Henry Jenkins. Retrived from [Http://Henryjenkins.Org/2010/02/\\_children\\_and\\_young\\_people.Html](Http://Henryjenkins.Org/2010/02/_children_and_young_people.Html),
- Jenkins, H., Purushotma, R., Weigel, M., Clinton, K. & Robison, A. J. (2009). *Confronting the challenges of participatory culture: media education for the 21st century*. Cambridge: Mit Press.
- Kumar, A., Pandey, S. N., Pareek, V., Faiq, M. A., Khan, N. I. & Sharma, V. (2017). Psychobiological determinants of 'Blue whale suicide challenge' victimization: a proposition for the agency mediated mental health risk in new media age. PsyArXiv, Sept.
- Kuss, D. J., Griffiths, M. D. & Binder, J. F. (2013). Internet addiction in students: prevalence and risk factors. *Computers in Human Behavior*, 29(3), 959-966.
- Kvavik, R. B. (2005). Convenience, communications, and control: how students use technology. *Educating the Net Generation*, 1, 7-20.
- Kwon J., Lee J., Lee H. (2011) Hidden Bot Detection by Tracing Non-human Generated Traffic at the Zombie Host. In: Bao F., Weng J. (eds) *Information Security Practice and Experience*. ISPEC 2011. Lecture Notes in Computer Science, vol 6672. Springer, Berlin, Heidelberg.
- Lazzaro, F. M. (2013). *L'Agenda digitale per l'Italia: l'amministrazione pubblica e le nuove sfide digitali*. Milano: Gruppo Wolters Kluwer.
- Lévy, M. (1997). *Computer-assisted language learning: Context and conceptualization*. Londo: Oxford University Press.

- Lévy, P. (1996). *L'intelligenza collettiva: per un'antropologia del cyberspazio* (2. ed.). Milano: Feltrinelli.
- Li, Y. & Ranieri, M. (2010). Are «digital natives» really digitally competent? A study on chinese teenagers. *British Journal of Educational Technology*. doi: 10.1111/j.1467-8535.2009.01053.x.
- Limburg, V. E. (1989). The decline of broadcast ethics: U.S. v. NAB. *Journal of Mass Media Ethics*, 4(2), 214-231. doi:10.1080/08900528909358345.
- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the Internet: The perspective of European children: Full findings and policy implications from the EU kids online survey of 9–16 year olds and their parents in 25 countries*. London: EU Kids Online Network Retrieved from [http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/EUKidsOnlineIIReports/D4FullFindings.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf).
- Lorenzo, G. & Dziuban, C. (2006). *Ensuring the Net Generation is net savvy*. Washington, DC: EDUCAUSE. Retrived from <http://www.educause.edu/ir/library/pdf/ELI3006.pdf>
- Magni, F. (2016). Le scuole paritarie e la legge 107/2015. *Nuova Secondaria*, 33(8), 27-32.
- Martin, A. & Grudziecki, J. (2006). DigEuLit: Concepts and Tools for Digital Literacy Development. *ITALICS: Innovations in Teaching & Learning in Information & Computer Sciences*, 5(4), 1-19.
- Marzuoli, C. (2002). Istruzione e "Stato sussidiario". *Diritto Pubblico*, 8(1), 117-160.
- Matteucci, N. (2015). La valutazione delle agende digitali regionali: un modello per gli investimenti pubblici in banda larga. *L'Industria*, 36(4), 551-582.
- McMahon, M. (2014). A Multidimensional Approach to Understanding and Addressing Digital Literacy in Higher Education. Paper presented at the The Higher Education Research and Development Society of Australasia (HERDSA) Conference 2014, Hong Kong.
- Mereu, M. G. & Franceschetti, M. (2017). Professioni nell'ICT: evidenze e prospettive. *Sinapsi*, 7, n. 2-3, pp. 87-117.
- Messi, G. (1992). Virus informatici: natura e rimedi. *Ratio Mathematica*, 4(1), 161-168.

- Midoro, V. (2007). Quale alfabetizzazione per la società della conoscenza. *TD–Tecnologie didattiche*, 41(2), 47–54. Retrived from:  
[http://www.itd.cnr.it/tdmagazine/PDF41/8\\_Midoro\\_TD41.pdf](http://www.itd.cnr.it/tdmagazine/PDF41/8_Midoro_TD41.pdf)
- Nancarrow, M. & Rifkin, W. (2011). *Reflective cycles and reflexive learning principles: teaching ethics from the learner outward*. (pp. 387-412) IGI Global. doi:10.4018/978-1-61350-510-6.ch023 Retrieved from <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84899383659&partnerID=40&md5=21fe20a58203d9c107a4f6b56298860c>
- National centre for technology in education (ncte) analisi del sondaggio del progetto dott.safe farrell grant sparks consulting. Retrieved from <https://docplayer.it/7615181-National-centre-for-technology-in-education-ncte-analisi-del-sondaggio-del-progetto-dot-safe-farrell-grant-sparks-consulting.html>
- Nocera, S. & Tagliani, N. (2015). *La normativa inclusiva nella nuova legge di riforma sulla “buona scuola”*. Vicalvi: Key.
- Olivieri, N. (2012). *Stimatori della media di una popolazione per dati mancanti*. (Tesi di laurea in statistica e gestione delle imprese) Università degli Studi di Padova, Italia.
- Paige, R., Hickok, E. & Patrick, S. (2004). *Toward a new golden age in american education: how the internet, the law, and today’s students are revolutionizing expectations*. Washington DC: US Department of Education, Office of Educational Technology.
- Parisi, M. (2011). Formazione civile e formazione religiosa: la questione delle “scuole di tendenza” e l’Islam. *Stato, Chiese E Pluralismo Confessionale. Rivista telematica*. Aprile. Retrived from <https://www.statoechiese.it>
- Parlamento Europeo (2006). Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry [Gazzetta Ufficiale L 378 del 27.12.2006]. Retrived from:  
[http://europa.eu/legislation\\_summaries/audiovisual\\_and\\_media/124030a\\_en.htm](http://europa.eu/legislation_summaries/audiovisual_and_media/124030a_en.htm)
- Peterlongo, P., Recla, M., Ventura, L., Centonze, M., & Torri, E. (2010). *Risorse umane. In Management in radiologia*. Milano: Springer, 287-304.

- Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the Horizon*, 9(5), 1-6.
- Prensky, M. R. (2012). *From digital natives to digital wisdom: Hopeful essays for 21st century learning*. Thousand Oaks: Corwin Press.
- Pérez-Tornero, J. (2004). *Promoting digital literacy: Understanding digital literacy*. (Final report EAC/76/03). Barcelona, Spain: UAB. Retrieved from: [http://ec.europa.eu/education/archive/elearning/doc/studies/dig\\_lit\\_en.pdf](http://ec.europa.eu/education/archive/elearning/doc/studies/dig_lit_en.pdf)
- Presidenza del Consiglio dei Ministri, (2003) *Ufficio studi per l'innovazione e le tecnologie*. Roma: Istituto Poligrafico e Zecca dello Stato S.p.A.
- Rivoltella, P.C., Ferrari, S. (eds.) (2010). *A scuola con i media digitali*. Milano, IT:
- Rivoltella, P.C. (2006). *Screen Generation. Gli adolescenti e le prospettive dell'educazione nell'età dei media digitali*. Milano: Vita&Pensiero.
- Rivoltella, P.C. (ed.). (2008). *Digital Literacy. Tools and methodologies for information society*. Hershey, PA: IGI.
- Rivoltella, P.C., & Ferrari, S. (eds.). (2010). *A scuola con i media digitali. Problemi, didattiche, strumenti*. Milano: Vita&Pensiero.
- Rivoltella, P. C., & Ferrari, S. (2014). *Scuola del futuro?: Appunti di una ricerca-intervento sull'innovazione tecnologica della didattica*. Milano: EDUCatt-Ente per il diritto allo studio universitario dell'Università Cattolica.
- Roncaglia, G. (2013). L'uso degli e-book nella formazione e nella didattica: tre riflessioni sugli e-book e sul loro ruolo. *La Vita Scolastica*, 67(10), 1–12.
- Rossi, P. G. (2014). Le tecnologie digitali per la progettazione didattica. *Journal of Educational, Cultural and Psychological Studies (ECPS Journal)*, (10), 113-133.
- Sammons, J. & Cross, M. (2017). *The Basics of Cyber Safety*. Amsterdam: Elsevier, 87-116.
- Signore, M., Carbini, R., D'Orazio, M., Brancato, G. & Simeoni, G. (2010, May). *Assessing Quality through Auditing and Self-assessment*. In European Conference on Quality in Official Statistics (Q2010), (4-6).

- Silverstone, R. (2005) Domesticating Domestication. Reflections on the Life of Concept (229-248), in T. Berker, M. Hartmann, M., Y. Punie and K. Ward (eds) *Domestication of Media and Technologies*. Maidenhead: Open University Press.
- Tambini, D. (2017). *Fake news: Public policy responses. Media policy brief 20*. London: Media Policy Project, London School of Economics and Political Science. Retrived from <https://goo.gl/6dvMtT>.
- Thiene, A. & Marescotti, E. (2017). Presentazione del numero monografico "la scuola al tempo dei social network". *Annali Online della Didattica e della Formazione Docente*, 9(13), 4-6.
- Tonioni, F. (2014). *Cyberbullismo: come aiutare le vittime e i persecutori*. Milano: Mondadori.
- Trentin, G. (2001). *Dalla formazione a distanza all'apprendimento in rete*. Milano: FrancoAngeli.
- Tullini, P. (2015). C'è lavoro sul web? *Labour & Law Issues*, 1(1), 1-20.
- Ventura, S. (1998). *La scuola tra Stato e Chiesa: la regolamentazione della scuola privata in Italia e in Francia*. Rimini: Maggioli Editore.
- Vese, D. (2016). Brevi riflessioni sul diritto alla cultura e la logica di mercato nella legge 13 luglio 2015, n. 107 (cd riforma della buona scuola). *Amministrativ@ Mente*, (5-6) Retrived from [www.amministrativamente.com](http://www.amministrativamente.com)
- Wolf, M., Barzillai, M., & Dunne, J. (2009). *The importance of deep reading. Challenging the whole child: Reflections on best practices in learning, teaching, and leadership*. Canada: ASCD Book.
- Zanetti, M. A. & Colangelo, R. M. (2018). Educare per prevenire la sofferenza delle cybervittime. Ricadute educative a partire dalla legge 71/2017. *Maltrattamento e abuso all'infanzia*, 1, 11-30.

## WEBGRAFÍA

[https://www.iene.mediaset.it/video/viviani-blue-whale-suicidarsi-per-gioco\\_97342.shtml](https://www.iene.mediaset.it/video/viviani-blue-whale-suicidarsi-per-gioco_97342.shtml)

<https://www.themoscowtimes.com/2017/07/19/founder-online-blue-whale-suicide-group-sentenced-a58446>

[https://www.ilmessaggero.it/news/esteri/blue\\_whale\\_philipp\\_budeikin\\_arrestato-2440986.html](https://www.ilmessaggero.it/news/esteri/blue_whale_philipp_budeikin_arrestato-2440986.html)

[Www.Digitalcompetence.Org/Moodle](http://Www.Digitalcompetence.Org/Moodle)

[Www.Washingtonpost.Com/News/Answer-Sheet/Wp/2018/03/27/Not-Sure-Whats-Real-Or-Fake-Anymore-The-News-Literacy-Project-Teaches-Kids-How-To-Tell-The-Difference-And-Its-Growing-Faster-Than-Ever/?Noredirect=On&Utm\\_Term=.Aa6c6d35c77b](http://Www.Washingtonpost.Com/News/Answer-Sheet/Wp/2018/03/27/Not-Sure-Whats-Real-Or-Fake-Anymore-The-News-Literacy-Project-Teaches-Kids-How-To-Tell-The-Difference-And-Its-Growing-Faster-Than-Ever/?Noredirect=On&Utm_Term=.Aa6c6d35c77b)

[Www.Wnyc.Org/Story/Breaking-News-Consumers-Handbook-Pdf/](http://Www.Wnyc.Org/Story/Breaking-News-Consumers-Handbook-Pdf/)

[Www.Mercurynews.Com/2018/03/27/News-Literacy-Project-Tackles-Fake-News-And-Business-Is-Booming/](http://Www.Mercurynews.Com/2018/03/27/News-Literacy-Project-Tackles-Fake-News-And-Business-Is-Booming/)

[Www.Ed.Stanford.Edu/News/Stanford-Researchers-Find-Students-Have-Trouble-Judging-Credibility-Information-Online](http://Www.Ed.Stanford.Edu/News/Stanford-Researchers-Find-Students-Have-Trouble-Judging-Credibility-Information-Online)

[Www.Ilpost.It/2018/12/11/Il-Piano-Dellunione-Europea-Contro-Le-Fake-News-Fa-Acqua/](http://Www.Ilpost.It/2018/12/11/Il-Piano-Dellunione-Europea-Contro-Le-Fake-News-Fa-Acqua/)

[Www.Repubblica.It/Tecnologia/2012/05/08/News/Se\\_Non\\_Paghi\\_Il\\_Prodotto\\_Sei\\_Tu\\_Quno\\_Vali\\_Sui\\_Social\\_Network\\_-34695300/](http://Www.Repubblica.It/Tecnologia/2012/05/08/News/Se_Non_Paghi_Il_Prodotto_Sei_Tu_Quno_Vali_Sui_Social_Network_-34695300/)

[Www.Childrenscommissioner.Gov.Uk/Publication/Growing-Up-Digital/](http://Www.Childrenscommissioner.Gov.Uk/Publication/Growing-Up-Digital/)

[Www.Tes.Com/Teaching-Resources/Digital-Citizenship](http://Www.Tes.Com/Teaching-Resources/Digital-Citizenship)

[Www.Digikomp.At/](http://Www.Digikomp.At/) [Https://](https://)

[Www.Betterinternetforkids.Eu/Web/Austria/Profile](http://Www.Betterinternetforkids.Eu/Web/Austria/Profile)

[Www.vublsts.wordpress.com/2016/07/29/the-european-handbook-for-teaching-privacy-and-data-protection-at-schools/](http://Www.vublsts.wordpress.com/2016/07/29/the-european-handbook-for-teaching-privacy-and-data-protection-at-schools/)

[Www.edri.org/papers/privacy-for-kids/](http://www.edri.org/papers/privacy-for-kids/)

[Www.communityhelpingschools.org/](http://www.communityhelpingschools.org/)

[Www.betterinternetforkids.eu/web/luxembourg/profile](http://www.betterinternetforkids.eu/web/luxembourg/profile)

[Www.betterinternetforkids.eu/hu/web/portal/](http://www.betterinternetforkids.eu/hu/web/portal/)

[Www.mediawijzer.net/](http://www.mediawijzer.net/)

[Www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=716671](http://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=716671)

[Www.childnet.com/resources/trust-me](http://www.childnet.com/resources/trust-me)

[Www.europarl.europa.eu/factsheets/it/sheet/138/politica-audiovisiva-e-dei-media](http://www.europarl.europa.eu/factsheets/it/sheet/138/politica-audiovisiva-e-dei-media)

[Www.linuxfocus.org/Italiano/September2002/article255.shtml](http://www.linuxfocus.org/Italiano/September2002/article255.shtml)

[Www.ottimizzazione-pc.it/i-tipi-di-malware-piu-diffusi/#](http://www.ottimizzazione-pc.it/i-tipi-di-malware-piu-diffusi/#)

[Www./nonaccademico.blogspot.it/2013/08/virus-informatici-cosa-sono-da-dove.html](http://www.nonaccademico.blogspot.it/2013/08/virus-informatici-cosa-sono-da-dove.html)

[Www.secoloditalia.it/2017/05/la-risposta-al-blue-whale-21-regole-della-balena-felice-boom-tra-i-giovani](http://www.secoloditalia.it/2017/05/la-risposta-al-blue-whale-21-regole-della-balena-felice-boom-tra-i-giovani)

[www.anp.it/competenze-chiave-nuova-raccomandazione-del-consiglio-deuropa/](http://www.anp.it/competenze-chiave-nuova-raccomandazione-del-consiglio-deuropa/)

[www.kidsmart.org.uk/](http://www.kidsmart.org.uk/)

[Www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/)

[Www.digizen.org/about.aspx](http://www.digizen.org/about.aspx), <https://www.childnet.com/>, <https://www.saferinternet.org.uk/>

[Www.eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:IT:PDF](http://www.eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:IT:PDF) (pp. 13-14)

<https://www.generazioniconnesse.it/site/it/il-progetto/>

[Www.ascuoladiopencoesione.it/](http://www.ascuoladiopencoesione.it/)

[Www.samsung.com/it/aboutsamsung/sustainability/corporate-citizenship/education/smart-school/](http://www.samsung.com/it/aboutsamsung/sustainability/corporate-citizenship/education/smart-school/)

[Www.facebook.com/insegnantiduepuntozero/](http://www.facebook.com/insegnantiduepuntozero/)

[Www.iltabletascuola.it/](http://www.iltabletascuola.it/)



[Www.mondodigitale.org/it/chi-siamo\\_temp](http://Www.mondodigitale.org/it/chi-siamo_temp)

[Www.betterinternetforkids.eu/](http://Www.betterinternetforkids.eu/)

[Www.saferinternet.org.uk/](http://Www.saferinternet.org.uk/)

[Www.safenet.bg/en/](http://Www.safenet.bg/en/)

[Www.betterinternetforkids.eu/web/greece/profile](http://Www.betterinternetforkids.eu/web/greece/profile)

[Www.betterinternetforkids.eu/web/slovenia/sid](http://Www.betterinternetforkids.eu/web/slovenia/sid)

[Www.saferinternet.org.uk/](http://Www.saferinternet.org.uk/)

[Www.ischool.startupitalia.eu/education/60619-20170801-pnsd-la-tabella-marcia-della-scuola-digitale](http://Www.ischool.startupitalia.eu/education/60619-20170801-pnsd-la-tabella-marcia-della-scuola-digitale)

[Www.agid.gov.it/agenda-digitale/agenda-digitale-italiana.](http://Www.agid.gov.it/agenda-digitale/agenda-digitale-italiana)

[Www.agid.gov.it/notizie/2017/04/07/pubblicate-gazzetta-ufficiale-misure-minime-sicurezza-informatica-pa](http://Www.agid.gov.it/notizie/2017/04/07/pubblicate-gazzetta-ufficiale-misure-minime-sicurezza-informatica-pa)

[Www.irishexaminer.com/ireland/most-teachers-feel-unequipped-to-teach-online-safety-463234.html](http://Www.irishexaminer.com/ireland/most-teachers-feel-unequipped-to-teach-online-safety-463234.html)

[Www.ilgiornale.it/news/cronache/foto-troppo-sexy-su-facebook-prof-si-dimette-1406363.html](http://Www.ilgiornale.it/news/cronache/foto-troppo-sexy-su-facebook-prof-si-dimette-1406363.html)

[Www.unicef.org/endviolence/endviolenceonline/](http://Www.unicef.org/endviolence/endviolenceonline/)

[Www.childnet.com/our-projects/project-deshame](http://Www.childnet.com/our-projects/project-deshame)

[Www.childnet.com/resources/pshetoolkit](http://Www.childnet.com/resources/pshetoolkit)

[www.betterinternetforkids.eu/web/esafety-label](http://www.betterinternetforkids.eu/web/esafety-label)

[Www.fondazioneveronesi.it/magazine/articoli/pediatria/navigare-sicuri-10-consigli-i-genitori-10-i-ragazzi](http://Www.fondazioneveronesi.it/magazine/articoli/pediatria/navigare-sicuri-10-consigli-i-genitori-10-i-ragazzi)

[Www.commissariatodips.it/da-sapere/per-i-genitori/navigazione-sicura-e-consapevole-dei-minori-su-internet.html](http://Www.commissariatodips.it/da-sapere/per-i-genitori/navigazione-sicura-e-consapevole-dei-minori-su-internet.html)

[Www.gazzettaufficiale.it/eli/id/2017/06/03/17G00085/sg](http://Www.gazzettaufficiale.it/eli/id/2017/06/03/17G00085/sg)

[Www.orizzontescuola.it/argo-software-chiarisce-sua-posizione-merito-alla-sicurezza-del-proprio-registro-elettronico-sc/](http://www.orizzontescuola.it/argo-software-chiarisce-sua-posizione-merito-alla-sicurezza-del-proprio-registro-elettronico-sc/)

[Www.miur.gov.it](http://www.miur.gov.it)

[Www.ncbi.nlm.nih.gov/pubmed/18828554](http://www.ncbi.nlm.nih.gov/pubmed/18828554)

[Www.scopus.com/inward/record.uri?eid=2-s2.0-84951177855&partnerID=40&md5=3ab3ea6782a53644ab6da5be1ae64518](http://www.scopus.com/inward/record.uri?eid=2-s2.0-84951177855&partnerID=40&md5=3ab3ea6782a53644ab6da5be1ae64518)

[Www.ofcom.org.uk](http://www.ofcom.org.uk)

[Www.provincia.torino.gov.it](http://www.provincia.torino.gov.it)

[Www.scopus.com/inward/record.uri?eid=2-s2.0-78049240706&partnerID=40&md5=e6a602b1592521f0b350edf3d24ba176](http://www.scopus.com/inward/record.uri?eid=2-s2.0-78049240706&partnerID=40&md5=e6a602b1592521f0b350edf3d24ba176)

[Www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/EUKidsOnlineIIRreports/D4FullFindings. pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIRreports/D4FullFindings.pdf)

[W ww.ed http://www.itd.cnr.it/tmagazine/PDF41/8\\_Midoro\\_TD41.pdf](http://www.ed http://www.itd.cnr.it/tmagazine/PDF41/8_Midoro_TD41.pdf)

[ucase.edu/ir/library/pdf/ELI3006.pdf](http://ucase.edu/ir/library/pdf/ELI3006.pdf)

[Www.statoechiese.it](http://www.statoechiese.it)

[Www.iene.mediaset.it/video/viviani-blue-whale-suicidarsi-per-gioco\\_97342.shtml](http://www.iene.mediaset.it/video/viviani-blue-whale-suicidarsi-per-gioco_97342.shtml)

[Www.themoscowtimes.com/2017/07/19/founder-online-blue-whale-suicide-group-sentenced-a58446](http://www.themoscowtimes.com/2017/07/19/founder-online-blue-whale-suicide-group-sentenced-a58446)

[Www.ilmessaggero.it/news/esteri/blue\\_whale\\_philipp\\_budeikin\\_arrestato-2440986.html](http://www.ilmessaggero.it/news/esteri/blue_whale_philipp_budeikin_arrestato-2440986.html)

[Www.gazzettaufficiale.it/eli/id/2017/06/03/17G00085/sg](http://www.gazzettaufficiale.it/eli/id/2017/06/03/17G00085/sg)

## **ANEXOS**

### **Cuestionarios**



1. Cosa sono i programmi antivirus?

Indica una risposta:

Sono programmi volti a combattere e sradicare virus informatici

Sono programmi realizzati per migliorare ulteriormente le prestazioni del computer

Sono programmi fatti per proteggere le informazioni private sui social-network

Sono programmi progettati per distruggere altri programmi antivirus

2. Quale delle seguenti affermazioni descrive meglio il virus?

Indica una risposta:

Un programma che protegge il computer da hacker  Un programma che viene installato sul computer che controlla il vostro uso di Internet.

Un programma che è segretamente installato sul computer, fa copie di se stesso, consuma le risorse del computer e può bloccarne l'utilizzo

3. Quale delle seguenti affermazioni è un **cattivo** consiglio per la protezione dei dispositivi informatici?

Indica una risposta:

Aggiornare costantemente il software antivirus

Aprire gli allegati nelle e-mail che si giudicano interessanti  Scaricare files solo da siti affidabili

4. Si dovrebbe tenere aggiornato il computer con l'ultima versione del sistema operativo perché...

Indica una risposta:

il download del software più recente renderà il computer più veloce

se non si dispone del software più recente, il sistema può costringerti a riavviare

gli hacker potrebbero approfittare di un bug o di una debolezza nota, del vecchio sistema, e infettarlo con un virus

5. Fin quando il software antivirus, sul proprio computer, è aggiornato nessun virus può infettarlo

Vero

Falso

6. Se il computer ha un software antivirus preinstallato all'acquisto, non si ha bisogno di comprare altri antivirus per proteggere il proprio computer

Vero. Il software antivirus preinstallato sul computer deve essere solo attivato e proteggerà il computer per tutto il tempo che rimarrà in uso

Falso. Il software antivirus preinstallato di solito è una versione di prova di 60-90 giorni, e ti verrà chiesto di acquistarlo, prima della scadenza, per continuare la protezione del tuo computer

7. Quali dei seguenti è un buon modo per creare una password?

Indica una risposta:

Utilizzare le informazioni personali come i derivati del proprio ID utente, i nomi dei membri della famiglia, delle automobili possedute, i numeri di targa, di telefono, i nomi degli animali domestici, i compleanni o gli indirizzi

Usare parole comuni prese dal dizionario

Creare una combinazione di lettere maiuscole e minuscole associate a numeri e simboli

1. Il primo passo per proteggersi dai rischi informatici è essere in grado di \_\_\_\_\_ una minaccia alla sicurezza. Indica una risposta:  evitare  sfidare

riconoscere

combattere

2. Una volta pubblicato un contenuto su Internet rimane sempre una sua traccia, anche se lo si elimina  Vero  Falso

3. Biblioteche, alberghi e altri luoghi pubblici hanno un computer per uso pubblico. Si consiglia di utilizzare questi computer per accedere ad informazioni personali o finanziarie (come un conto corrente).

Vero  Falso

4. Il **Cyber bullismo** può avvenire attraverso il computer, i telefoni cellulari e i tablet.  Vero  Falso

5. Cos'è un **malware**? Indica una risposta:

Un Malware è costituito solo da worm

Un Malware è costituito solo da trojan

Un Malware è costituito solo da virus

Un Malware è costituito da tutti e tre, virus, worm e trojan

6. Qual'è il modo migliore per utilizzare i social network? Indica **due** risposte:


Contare su impostazioni di sicurezza predefinite

Impostare la privacy e le impostazioni di sicurezza in base al proprio livello di comfort personale per la condivisione delle informazioni

Evitare la condivisione di foto compromettenti e informazioni personali

7. Paolo Rossi sta utilizzando Mozilla Firefox come browser

L'icona, riportata sopra, indica che sta effettuando una navigazione in

incognito?   Vero  Falso

8. Stai leggendo la tua posta elettronica su un computer pubblico (a scuola, in albergo,...) prima di chiudere il browser utilizzi l'opzione "ricorda password"?  No

Si

9. Cos'è il **phishing**?

Un modo con cui le banche tentano di attirare clienti  Un metodo per proteggersi da furti di identità e frodi on-line  Una email-truffa condotta al fine di rubare informazioni o identità

1. Quale delle seguenti associazioni rappresenta le **tre R dei rifiuti**? Indica una risposta:

Ridurre - Rispettare - Riciclare

Ridurre - Riutilizzare – Riciclare

Ridurre - Riconsiderare - Rispettare

2. Perché i dispositivi elettronici sono considerati pericolosi?

Indica una risposta:  Perché si degradano, nel tempo, rilasciando nell'aria sostanze chimiche cancerogene

Perché rilasciano metalli tossici che possono confluire nelle discariche e nelle acque sotterranee

Perché il piombo e il mercurio presente nei loro componenti può causare cambiamenti metabolici negli utenti

3. Cosa si intende per **e-waste**? Indica una risposta:

Rifiuti chimici pericolosi

Rifiuti derivanti dalla produzione di energia nucleare  Apparecchiature elettroniche obsolete  Rifiuti ecologici

4. Qual'è l'opzione meno utile per la gestione dei rifiuti?

Riutilizzo

Recupero

Smaltimento

1. Quale problema di salute può causare digitare sulla tastiera di un computer, per ore, ogni giorno? Indica una risposta:

Malattie del cuore  Problemi alla schiena

Lesioni da sforzo ripetitivo (RSI)

2. Quali problemi può causare lo sfarfallio di uno schermo? Indica una risposta:

Lesioni da sforzo ripetitivo

(RSI)  Problemi alla schiena

Affaticamento degli occhi

3. Quando si lavora alla scrivania, la testa e il collo dovrebbero essere in linea con il

busto.  Vero  Falso

4. Il monitor del computer dovrebbe essere leggermente più alto rispetto al livello degli occhi

Vero

Falso

<p>5. Come si possono ridurre i rischi per la salute causati da un uso prolungato del computer?</p> <p><input type="checkbox"/> Fare esercizi frequentemente</p> <p><input type="checkbox"/> Avere regolari periodi di riposo dallo schermo</p> <p><input type="checkbox"/> Predisporre una posizione di lavoro confortevole <input type="checkbox"/> Tutte quelle menzionate</p>
<p>6. Come si può mantenere un equilibrio fra il mondo virtuale (sul computer) e quello reale?</p> <p><input type="checkbox"/> Trascorrere del tempo con gli amici</p> <p><input type="checkbox"/> Predisporre un tempo specifico per socializzare su internet, trascorso il quale scollegarsi</p> <p><input type="checkbox"/> Entrambe</p>
<p>1. Vuoi prenotare on line il biglietto per un concerto rock. Hai saputo che non solo si può prenotare ma che si può pagare direttamente on line. Cosa ne pensi? (indica una risposta)</p> <p><input type="checkbox"/> È possibile pagare on line, utilizzando la carta di credito, su siti che adottano un certo tipo di protezione <input type="checkbox"/> Non credo sia possibile pagare on line <input type="checkbox"/> È possibile pagare on line, ma occorre conoscere di persona il venditore <input type="checkbox"/> È possibile pagare on line, ma è meglio evitare di farlo</p>
<p>2. La tua scuola ha creato un sito Internet nel quale sono presenti anche i dati degli studenti. Ti chiedono di scrivere una serie di informazioni (data di nascita, classe frequentata, interessi personali, una tua foto). Nello stesso periodo ti sei anche registrato ad una chat di discussione libera, esterna al sito della scuola, nella quale ti viene chiesto di inserire le stesse informazioni. Come ti comporti? (indica una risposta) Inserisci i tuoi dati personali:</p> <p><input type="checkbox"/> in entrambi i casi <input type="checkbox"/> solo nel secondo caso (chat pubblica) <input type="checkbox"/> solo nel primo caso (sito della scuola)</p>
<p>3. In Internet si sta diffondendo sempre di più il fenomeno dell'inserimento di audio, video e fotografie personali, all'interno di siti web, da cui possono essere visti, ascoltati e scaricati da chiunque. Tra i problemi che questo fenomeno solleva, indicati qui sotto, qual'è, a tuo avviso, quello di più difficile soluzione?</p> <p>Rispetto delle clausole d'uso stabilite dagli autori</p> <p>Titolazione e commento dei materiali da parte di chi accede al sito <input type="checkbox"/> Riproduzione dei materiali digitali scaricati <input type="checkbox"/> Inserimento/scaricamento di materiali nel sito</p>
<p>4. Roberto, nel suo blog, prende in giro i difetti fisici di Mario e invita gli amici che lo conoscono a fare altrettanto. Secondo te: (indica una risposta) <input type="checkbox"/> è accettabile solo perché si è tra ragazzi <input type="checkbox"/> non approvi il suo atteggiamento, ma partecipi anche tu allo scherzo <input type="checkbox"/> si tratta da uno scherzo, non c'è nulla di male <input type="checkbox"/> è un comportamento del tutto inaccettabile</p>
<p>5. Fai un video ai tuoi compagni e lo metti su Internet. E' un comportamento accettabile?</p> <p><input type="checkbox"/> Sì. Tra ragazzi si può fare</p> <p><input type="checkbox"/> Sì. Se lo scarico da casa nessuno sa chi lo ha messo su Internet</p> <p><input type="checkbox"/> No. Per mettere il video in Internet dovrei chiedere il permesso a ciascun compagno</p>

<input type="checkbox"/> No. Non si scaricano video su internet				
6. Ricevi un messaggio di posta elettronica (e-mail) in cui vieni invitato ad una festa nella tua città ad un indirizzo che non conosci. Che cosa fai?				
<input type="checkbox"/> Non accetto l'invito perchè non conosco le persone <input type="checkbox"/> Accetto ma dopo aver chiesto più informazioni sul tema della festa <input type="checkbox"/> Accetto l'invito, sono curioso e voglio divertirmi <input type="checkbox"/> Chiedo il parere di qualche amico				
7. Tuo nonno ha dei risparmi depositati nella Banca XX. Riceve una e-mail che riporta il nome della BancaXX in cui gli richiedono di indicare via e-mail i codici di accesso e le password, perchè la Banca deve fare un controllo . Cosa gli consigli?				
<input type="checkbox"/> Di fornire i dati se nel messaggio c'è il nome del Direttore della Banca <input type="checkbox"/> Di fornire i dati se nell'email c'è il logo della Banca <input type="checkbox"/> Di non rispondere, aggiungere allo spam e, in caso, avvisare la polizia <input type="checkbox"/> Di fornire i dati, se conoscono il suo indirizzo e-mail, sono i dipendenti della sua Banca				
8. Un bambino di 8 anni, che sa già usare il computer, chiede di poter navigare liberamente in Internet. Qual'è la tua opinione?				
<input type="checkbox"/> Se è capace di usare Internet, deve essere libero di andarci <input type="checkbox"/> Gli va detto di evitare i siti troppo complicati per lui <input type="checkbox"/> A navigare in Internet si perde troppo tempo <input type="checkbox"/> Ci sono siti che non sono adatti a lui				
9. In un sito internet leggi che se inserisci i tuoi dati personali, riceverai a casa un gioco, un tablet o un nuovo cellulare. Cosa fai?				
<input type="checkbox"/> Non inserisco i dati perchè non so come possono essere usati <input type="checkbox"/> Inserisco i dati personali perchè tanto non mi costa niente <input type="checkbox"/> Non inserisco i dati personali perchè possono andare persi <input type="checkbox"/> Inserisco i dati solo se viene indicato il nome di chi me li chiede				
Età _____ Sesso <input type="checkbox"/> M <input type="checkbox"/> F Classe frequentata _____				
Ore giornaliere trascorse su internet con il computer _____, con il tablet _____, con il cellulare _____				
Sensazione percepita del rischio che si corre su internet				
<input type="checkbox"/> Nullo	<input type="checkbox"/> Scarso	<input type="checkbox"/> Medio	<input type="checkbox"/> Alto	<input type="checkbox"/> Molto Alto
Libertà di utilizzare il cellulare in classe				
<input type="checkbox"/> Nulla	<input type="checkbox"/> Scarsa	<input type="checkbox"/> Media	<input type="checkbox"/> Alta	<input type="checkbox"/> Molto alta
Tempo dedicato alla navigazione su Internet durante le ore di lezione				



Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
Esprimi un'opinione personale sulla sicurezza in Internet e sull'uso dei cellulari a scuola da parte degli studenti				



VNIVERSITAT  
ID VALÈNCIA

Departament de Didàctica i Organització Escolar Facultat de Filosofia i CC.  
Educació València - *All Rights Reserved* – Ricerca dottoranda Tiziana  
Occhipinti

Età \_\_\_\_\_ Sesso M F Classi in cui si sta insegnando \_\_\_\_\_  
materie insegnate \_\_\_\_\_

Secondo te, che grado di rischio percepiscono di correre, gli studenti, navigando in Internet?

<input type="checkbox"/> Nullo	<input type="checkbox"/> Scarso	<input type="checkbox"/> Medio	<input type="checkbox"/> Alto	<input type="checkbox"/> Molto Alto
--------------------------------	---------------------------------	--------------------------------	-------------------------------	-------------------------------------

Che libertà hanno, gli studenti, di utilizzare il cellulare in classe?

<input type="checkbox"/> Nulla	<input type="checkbox"/> Scarsa	<input type="checkbox"/> Media	<input type="checkbox"/> Alta	<input type="checkbox"/> Molto alta
--------------------------------	---------------------------------	--------------------------------	-------------------------------	-------------------------------------

Quanto tempo, gli studenti, dedicano alla navigazione in Internet per motivi didattici?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, sono informati dell'esistenza di programmi per la sicurezza dei dispositivi informatici?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

...se conoscono i programmi sulla sicurezza informatica, secondo te, li utilizzano?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, sanno proteggere la loro salute dall'uso eccessivo del computer?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, conoscono quei comportamenti di smaltimento dei dispositivi informatici che proteggono l'ambiente?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

...se li conoscono, secondo te, li mettono in pratica?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, sanno che i dati personali diffusi su internet possono essere rubati?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

... se lo sanno, mettono in pratica dei comportamenti che salvaguardano i loro dati personali?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Esprimi un'opinione personale sulla sicurezza in Internet e sull'uso dei cellulari a scuola da parte degli studenti

---



---



---



---



---



---



Genitori: Età \_\_\_\_\_ Sesso M F classe frequentata dal figlio/a \_\_\_\_\_

Secondo te, che grado di rischio percepiscono di correre, gli studenti, navigando in Internet?

<input type="checkbox"/> Nullo	<input type="checkbox"/> Scarso	<input type="checkbox"/> Medio	<input type="checkbox"/> Alto	<input type="checkbox"/> Molto Alto
--------------------------------	---------------------------------	--------------------------------	-------------------------------	-------------------------------------

Che libertà hanno, gli studenti, di utilizzare il cellulare in classe?

<input type="checkbox"/> Nulla	<input type="checkbox"/> Scarsa	<input type="checkbox"/> Media	<input type="checkbox"/> Alta	<input type="checkbox"/> Molto alta
--------------------------------	---------------------------------	--------------------------------	-------------------------------	-------------------------------------

Quanto tempo, gli studenti, dedicano alla navigazione in Internet per motivi didattici?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, sono informati dell'esistenza di programmi per la sicurezza dei dispositivi informatici?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

...se conoscono i programmi sulla sicurezza informatica, secondo te, li utilizzano?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, sanno proteggere la loro salute dall'uso eccessivo del computer?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, conoscono quei comportamenti di smaltimento dei dispositivi informatici che proteggono l'ambiente?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

...se li conoscono, secondo te, li mettono in pratica?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Secondo te, gli studenti, sanno che i dati personali diffusi su internet possono essere rubati?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

... se lo sanno, mettono in pratica dei comportamenti che salvaguardano i loro dati personali?

Molto poco	Poco	Abbastanza	Più che abbastanza	Molto (più che abbastanza)
------------	------	------------	--------------------	----------------------------

Esprimi un'opinione personale sulla sicurezza in Internet e sull'uso dei cellulari a scuola da parte degli studenti

---

---

---

---

---

---

---

---